TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

JARI SYRJÄLÄ

PILVIPALVELUIDEN TIETOSUOJAN VARMISTAMINEN

Diplomityö

Tarkastaja ja aihe hyväksytty talouden ja rakentamisen tiedekuntaneuvoston kokouksessa 4. kesäkuuta 2014.

TIIVISTELMÄ

JARI SYRJÄLÄ: Pilvipalveluiden tietosuojan varmistaminen
Tampereen teknillinen yliopisto
Diplomityö, 97 sivua
Maaliskuu 2015
Tietotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Ohjelmistotekniikka
Tarkastaja: Professori Pekka Loula

Avainsanat: pilviteknologia, tietosuoja, salausalgoritmi

Virtuaalisointiteknologian kehittyminen 1990-luvulta lähtien ja sen ulkoistaminen 2000-luvulla on mahdollistanut myymään tietojenkäsittelyä palveluna kuluttajille ja organisaatiolle. Pilviteknologia on mahdollistanut kuluttajille ja yrityksille kustannustehokkaat, laajennettavat ja helposti käyttöönotettavat palvelut. Palvelujen laajentaminen pilvialustoille on kuitenkin aiheuttanut kuluttajissa ja erityisesti yrityksissä lisääntyvässä määrin huolestuneisuutta tietoturvasta ja tietosuojasta.

Diplomityön tavoitteena oli selvittää suomalaisten pilvipalvelutuottajien tietosuojaan liittyviä teknisiä ratkaisuja suojata yritysten ja kuluttajien arkaluontoista tietoaineistoa erityisesti tietoturvan ja tietosuojan kehittämiseksi.

Johtopäätöksenä voidaan todeta, että tutkittavien case-tapausten osalta suomalaiset pilvipalvelut ovat fyysisen suojauksen, käytettävyyden ja saatavuuden osalta hyvällä tasolla sekä myös infrastruktuuri- ja sovellustietoturvan osalta. Työssä ei voitu kuitenkaan osoittaa miten hyvin tietosuojan varmistaminen on toteutettu pilvipalveluissa.

ABSTRACT

JARI SYRJÄLÄ: Securing confidentiality in Cloud Services
Tampere University of Technology
Master of Science Thesis, 97 pages
March 2015
Major: Software engineering
Examiner: Professor Pekka Loula

Keywords: cloud technology, data protection, encryption algorithm

The developing of the virtualization technology since 1990s and its outsourcing in the 21st century has provide to sell computing as a service for the customers and the organizations. A cloud technology have been made it possible for the customers and the companies provide more cost efficient and more expanded and easily deploying services than ever. Nevertheless expanded the services to the cloud platforms have produced for the customers and especially for the companies increasingly concern about the security and the data protection.

A master's thesis goal was investigated the Finnish cloud solution providers technical solution for the data protection to secure for the companies and the customers sensitive data especially to developing for the security and the data protection.

In conclusion we are able to state that the case studies which were study regarding to the Finnish cloud solution providers has a good level for the physical security and the usability and the availability and also concerning to the infrastructure and the application security. However in the master's thesis we are not able to point out how well the securing confidentiality have accomplished for the cloud services.

ALKUSANAT

Tämä diplomityö on tehty Tampereen teknillisen yliopiston Porin yksikössä. Haluan esittää parhaimmat kiitokset työn ohjaajalle ja tarkastajalle professori Pekka Loulalle arvokkaista neuvoista ja kannustuksesta työn loppuun saattamiseksi.

Lopuksi haluan kiittää aviopuolisoani Ulla Saarelaa ymmärryksestä ja tuesta tämän työn ja opintojeni aikana.

SISÄLLYSLUETTELO

KUVALUETTELO

TAULUKKO

LYHENTEET JA MERKINNÄT

AES – Advanced Encryption Standard on lohkosalausjärjestelmä, jossa viesti salataan ja puretaan samalla avaimella. AES voitti vuonna 2001 avoimen kansainvälisen kilpailun salausmenetelmänä. AESia käytetään nykyisin ympäri maailman ohjelmistoissa ja laitteistoissa salaamaan arkaluontoista dataa.

API - Application Program Interface - koodi, joka mahdollistaa kahden ohjelmiston kommunikoimaan toistensa kanssa

ACID (Atomicity, Consistency, Isolation, Durability) – on kirjainlyhenne atomisuudelle, eheydelle, eristyneisyydelle ja pysyvyydelle. ACID tarkoittaa tietokantajärjestelmien periaatetta, jonka avulla turvataan järjestelmän tietojen eheys kaikissa tilanteissa. Atomisuus tarkoittaa, että jokin tapahtuma suoritetaan joko kokonaan tai ei lainkaan. Eheys takaa, että tietokanta tapahtumien myötä siirtyy yhdestä eheästä tilasta toiseen eheään tilaan. Eristyneisyys takaa, että transaktiot eivät vaikuta toisiinsa ja toimivat kuin yksin järjestelmässä. Pysyvyys määrää, että tapahtuman sitoutumisen jälkeen muutokset eivät enää voi kadota järjestelmästä.

BGP - Border Gateway Protocol on internetin tärkein reititysprotokolla, jonka tehtävänä on hoitaa reititys autonomisten järjestelmien välillä.

BitTorrent - on sisällön jako protokolla joka mahdollistaa tehokkaan ohjelmistojakelun sekä erittäin suurten tiedostojen peer-to-peer jaon kuten elokuvien ja TV-ohjelmien

CaaS – Communication as a Service on ulkoistettu yrityksen kommunikointiratkaisu, joka voidaan vuokrata yksittäiseltä toimittajalta. Kommunikaatioratkaisu voi sisältää seuraavia palveluja kuten pikaviestinnän, äänen välittämisen hyödyntämällä internettiä, työryhmä- ja videokonferenssisovellukset joita voidaan käyttää esimerkiksi mobiililaitteilla.

DaaS - Data as a Service on informaation jakelumalli, jossa data-tiedostot (sisältäen tekstiä, kuvia, ääntä ja videoita) on tuotu saataville asiakkaille yli julkisen tietoverkon (internet).

DVDM-tekniikka - Dense Wavelength Division Multiplexing on optinen tekniikka jota käytetään kasvattamaan olemassa olevan valokuiturunkoverkon kaistaa. DMVM - tekniikassa yhdistetään ja siirretään useita signaaleja samanaikaisesti eri aallonpituuksilla samassa valokuitukaapelissa.

HaaS – Hardware as a Service on palvelumalli laitteistolle, joka on määritelty eritavalla hallinnoiduissa palveluissa ja pilvilaskenta kontekstissa. Hallinnoiduissa palveluissa asiakas maksaa pilvipalvelun tuottajalle kuukausittaisen maksun asiakkaalle tuotetuista palveluista. Hallinnoitu palvelumalli muistuttaa leasing-mallia. Pilvilaskennassa asiakas maksaa palvelusta tarve perusteisesti, jossa palvelun asiakas määrittelee miten dataa käsitellään pilvipalvelussa. Tällainen palvelu on esimerkiksi Amazon EC2.

Hilalaskenta - hajautettua ja rinnakkaista sovellusten suorittamista hilalaskentajärjestelmässä(engl. grid computing).

HIPAA - United States Health Insurance Portability and Accountability Act on yhdysvaltojen terveysvakuutuksen siirrettävyys- ja vastuullisuuslaki vuodelta 1996. HIPAA pyrkii vahvistamaan standardoidun mekanismin sähköiseen tietojen vaihtoon, tietoturvaan ja luottamuksellisuuteen kaikkeen terveystietoja koskevissa tietojen vaihdossa.

HITECH - The Health Information Technology for Economic and Clinical Health lainsäädäntö on luotu virkistämään sähköisen terveys tietueen (Electronic Health Record) käyttöönottoa ja sitä tukevaa teknologiaa yhdysvalloissa.

IaaS - Infrastructure as a Service tarkoittaa palvelimien ja palvelinsalien ulkoistamista. Kokonaisuuteen sisältyy yleensä verkkoyhteydet, tallennustila, palvelimet ja niiden ylläpito.

IP-transit – Internet Protocol transit helpottaa internet liikenteen siirtoa yhdistämällä pieniä verkkoja ja internet-operaattoreita suurempiin verkkoihin luotettavalla asiakas reitityksellä. IP-transit parantaa useita verkkotoimintoja kuten lataus- ja selailunopeutta.

KVM - Kernel-based Virtual Machine eli KVM on Linux-ytimeen rakennettu tuki virtualisoinnille. Se tukee tällä hetkellä täydellistä virtualisointia Intel VT:n ja AMD-V:n avulla sekä rajoitetusti paravirtualisointia Linux- ja Windows-asiakaskäyttöjärjestelmille.

Man-in-the-middle-attack - miesvälissä hyökkäys on menetelmä, joka mahdollistaa tunkeutujan pääsemään kiinni arkaluonteiseen tietoon sieppaamalla ja muuttamalla tietoliikennettä julkisen verkon käyttäjän ja minkä tahansa verkkosivun tai palvelun välillä.

Multitenanttisuus - tarkoittaa, että palvelun suorittamiseen vaadittavat laitteistoresurssit on jaettu kaikkien käyttäjien kesken sen sijaan, että jokaista käyttäjää kohden olisi oma dedikoitu fyysinen laitealusta tai ohjelmistonsa.

On-demand - tarkoittaa palvelua tai toimintaa, joka vastaa sen käyttäjän tai asiakkaan tarpeeseen tarvittaessa tai vaadittaessa. Yleensä on demand -palvelun arvo liittyy siihen, että palvelun tarjoaja tai kuluttaja ei joudu tekemään ennakkoon taloudellisia panostuksia, vaan maksu suoritetaan vain palvelua tai toimintoa käytettäessä, ja näin myös on demand -palvelut ovat niiden käyttäjille usein normaalia edullisempia.

OpenStack - avoimeen lähdekoodiin perustuva pilvialusta, jolla voidaan rakentaa IaaS pilvipalveluita. Se mahdollistaa pilven skaalautuvuuden sekä runsaasti ominaisuuksia esimerkiksi automaation avulla. OpenStack-projektin on alun perin käynnistänyt USA:n avaruushallinto NASA sekä Rackspace, ja se on nykyään ylivoimaisesti suurin avoin pilvialusta sekä yksi suurimmista käynnissä olevista avoimen lähdekoodin projekteista. OpenStackin tarkoituksena on mahdollistaa pilven ajaminen standardilaitteistolla. OpenStackin kehityksestä vastaa OpenStack Foundation. Sen takana kehittämässä ja rahoittamassa toimintaa on tällä hetkellä satoja yrityksiä, myös merkittävä määrä kansainvälisiä toimijoita kuten IBM, HP, Intel sekä Red Hat.

PaaS - Platform as a Service tarkoittaa palvelualustan ulkoistamista. Palvelualustan ulkoistaminen tuo mukanaan etuja sekä ohjelmistokehityksen että liiketoiminnan näkökulmasta.

PCI DSS - Payment Card Industry Data Security Standard on laajasti hyväksytty joukko politiikoita ja menettelyjä aikomuksena optimoida luotto- ja pankkikorttien tietoturvaa ja suojata luottokortinhaltijaa henkilötietojen väärinkäyttöä vastaan.

A public key infrastructure (PKI) - julkisen avaimen infrastruktuuri tukee julkisen salausavaimen jakamista ja tunnistamista mahdollistaen käyttäjien ja tietokoneiden tietoturvallisesti vaihtamaan tietoa yli julkisen verkon kuten internet ja varmentamaan toisen osapuolen identiteetin.

REST - Representational State Transfer on yksinkertainen tilaton arkkitehtuuri, jota yleisesti ajetaan sovelluskerroksella. REST lukee kohdennettua websivua, joka sisältää XML-tiedoston. REST käytetään usein mobiilisovelluksissa, sosiaalisessaverkossa ja automatisoiduissa prosesseissa.

Rich Client - verkkoon liitetty tietokone, jolle on asennettu paikallisesti joitakin tietokoneresursseja mutta on myös riippuvainen muista verkon hajautetuista resursseista.

RSA - epäsymmetrinen salausjärjestelmä, joka toteuttaa julkisen avaimen infrastruktuurin. RSA salaus pohjautuu julkisen ja yksityisen avaimen käyttöön. RSA-salausalgoritmin ovat kehittäneet Ron Rivest, Adi Shimar ja Len Adleman Massachusetts teknillisessä korkeakoulussa (MIT) vuonna 1977 ja se julkaistiin vuonna 1978.

SaaS - Software as a Service tarkoittaa ohjelmiston hankkimista palveluna perinteisen lisenssipohjaisen tavan sijasta. Käytöstä maksetaan yleensä käytön laajuuden mukaan.

SAS 70 Type II - Statement on Auditing Standards (SAS) No. 70 määrittelee ne standardit, joita auditoijan täytyy noudattaa arvioidessaan sopimuksen mukaisesti palveluorganisaation kuten esimerkiksi datakeskuksen sisäisiä prosesseja.

SOAP - Simple Object Access Protocol on tapa miten ohjelma ajetaan käyttöjärjestelmässä kuten Windows kommunikoimaan ohjelman kanssa samassa tai toisen tyyppisessä käyttöjärjestelmässä kuten Linux käyttämällä http-protokollaa ja XML:ää mekanismina tiedon vaihdossa.

SOX - joka tunnetaan yleisesti myös nimillä Public Company Accounting Reform and Investor Protection Act of 2002 ja SOX sekä SarbOX on Yhdysvaltain liittovaltion laki, joka asettaa määräyksiä kaikkien Yhdysvalloissa pörssinoteerattujen yritysten hallinnosta ja johtamisesta sekä tilintarkastusyhtiöiden toiminnasta.

SSL - Secure Socket Layer on tietoliikenneprotokolla, joka hoitaa palvelimen todentamisen, päätelaitteen todentamisen ja salaa tietoliikenteen palvelimen ja päätelaitteen välillä.

Tietoaineisto - tässä opinnäytetyössä tietoaineistolla tarkoitetaan tekstiä, kuvia, ääntä jne. Myös tietokantaan tallennettu aineisto.

VM – Virtual Machine ”virtuaalilaite” mahdollistaa täydellisen järjestelmäalustan, joka tukee käyttöjärjestelmän suoritusta. Tämä tavallisesti emuloi olemassa olevaa ohjelmisto- ja laitteistoarkkitehtuuria (muisti, tietoliikenne, prosessori ja niin edelleen) tarkoituksena antaa alustan ajettaville ohjelmille/sovelluksille missä todellinen laitteisto ei ole saatavilla.

VMM – Virtual Machine Monitor on isäntäohjelma, joka mahdollistaa yksittäisen tietokoneen tukemaan useita identtisiä suoritusympäristöjä. Käyttäjät näkevät järjestelmät itsenäisinä tietokoneina eristettynä toisistaan, vaikka kaikkia käyttäjiä palvellaan samalla koneella. Esimerkiksi IBM:n VM/ESA käyttöjärjestelmä voi kontrolloida useita virtuaalilaitteita IBM S/390 järjestelmällä.

Web Service - ovat palveluja (ohjelmien ja datan yhdistelmiä), jotka ovat saatettu saataville web-palvelimelta käyttäjille tai muille internettiin kytketyille ohjelmille.

XML - eXtensible Markup Language on kuvauskieli, jolla kuvataan tiedon merkitys sekä tieto itse.

1 JOHDANTO

Pilviteknologia on ajankohtainen ja maailmanlaajuisesti kiinnostusta herättänyt tutkimuskohde tietojenkäsittelytieteissä erityisesti tietoturvaan ja tietosuojaan liittyvissä osa-alueissa. Internetin ja web-teknologian sekä hajautettuja järjestelmiä ja virtuaalisointia yhdistävän teknologian kehittyminen on mahdollistanut ajasta ja paikasta riippumattomien tietotekniikkapalvelujen tarjoamisen kuluttajille ja yrityksille. Vaquero *et al.* (2009) mukaan pilvestä tarjottavat tietotekniikkapalvelut ovat kustannustehokkaita ja kustannukset muodostuvat käytettyjen palvelujen perusteella.

Pilviteknologian yhdistäessä aikaisempia teknologisia ratkaisuja on kehittynyt tietojenkäsittelyparadigma, jossa tietotekniikkaa myydään samalla tavalla hyödykkeenä kuin esimerkiksi energiateollisuus myy sähköä kuluttajille. Kustannustehokas, skaalautuva, helppokäyttöinen ja internetin yli tarjottava tietojenkäsittelyparadigma on nopeaa vauhtia yleistymässä globaalisti. Pilvipalveluiden tuottamiseen liittyvä luottamuksellisuus ja palveluiden saatavuus aiheuttaa kuitenkin tietoturvaan liittyviä kysymyksiä monessa pilvipalveluita hyödyntävässä organisaatiossa. Kolmannen osapuolen olemassaolo, tietojen hajauttamisesta aiheutuva tiedon kontrollin hämärtyminen ja teknologian kehittymättömyys ovat merkittäviä riskejä aiheuttavia uhkatekijöitä tietoturvalle ja -suojalle.

Pilvestä tarjottavien tietojenkäsittelypalveluiden lisääntynyt kasvu on lisännyt kuluttajissa ja yrityksissä huolestuneisuutta tietojen joutumisesta vääriin käsiin (Gadzheva 2008). Yrityssalaisuuksien ja henkilökohtaisten tietojen altistuessa erilaisille väärinkäytöksille, on tietosuoja vakavasti uhattuna. Gadzhevan (2008) mukaan tietojen suojaamiseen on alettu tästä syystä kiinnittää kasvavassa määrin huomioita yritysten hyödyntäessä hajautettuja teknologiapalveluita.

1.1 Tutkimuksen tavoite ja rajaus

Tämän diplomityön tavoite on selvittää case-tutkimuksen pohjalta suomalaisten pilvipalvelutuottajien tietosuojaan liittyviä teknisiä ratkaisuja suojata yritysten ja kuluttajien arkaluontoista tietoaineistoa erityisesti tietoturvan ja tietosuojan kehittämiseksi. Työssä käsitellään myös tarkemmin tietosuojan varmistamiseen liittyviä tietoturvaratkaisuja, algoritmeja sekä tähän liittyviä sovelluksia pilvipalveluiden tietosuojan varmistamiseksi. Hakala *et al.* (2006) mukaan tietoturva koostuu luottamuksellisuudesta, käytettävyydestä ja eheydestä. Tietosuoja on sen sijaan Järvisen (2003) mukaan ”henkilöön tai hänen toimintaansa liittyvien tietojen suojaamista luvatonta keräämistä ja käyttöä vastaan”.

Pilviteknologia koostuu erilaisista tietoteknisistä ratkaisuista, jotka ovat lähtökohta internetistä tarjottaville pilvipalveluille. Tämän diplomityön kannalta tärkeä asia on tietojenkäsittelyn ulkoistaminen ja siihen liittyvät riskit, tietojen suojaaminen ja tietojen valvonnan hämärtyminen. Tästä näkökulmasta lähtien tässä diplomityössä käsitellään erityisesti Software as a Service-pilvipalvelumallin tietoturvaa ja datan salaustekniikoita sekä toisaalta standardien merkitystä pilvipalveluiden tietoturvan ja tietosuojan kehittämiseksi.

Tässä diplomityössä haetaan vastauksia seuraaviin kysymyksiin:

- Miten hyvin tutkittavien suomalaisten pilvipalveluja tarjoavien toimijoiden tietoturvaan liittyvät ratkaisut turvaavat arkaluonteisen tietoaineiston pilvessä?
- Millaisia mahdollisuuksia on pilvipalvelua hyödyntävällä asiakkaalla varmistua ja kontrolloida itse pilveen tallennetun tietoaineiston tietosuojasta?
- Miten paljon tutkittavat pilvipalvelun tuottajat hyödyntävät ja noudattavat tietoturvastandardeja arkaluontoisen tietoaineiston suojaamiseksi pilvessä?

Henkilökohtaisten ja luottamuksellisten tietojen suojaaminen on erityisen tärkeää niin pilvipalveluita kehittävän kuin hankkivan tahon kannalta (Dey 2007). Tietoturvan ja tietosuojan rikkoontuminen on myös merkittävä riski liiketoiminnalle ja yksilöiden yk-

sityisyydelle (Tafti 2005). Näin ollen tietoturvan ja tietosuojan takaaminen ovat siis oleellisia riskienhallinnan osa-alueita.

Diplomityössä käsitellään myös suppeasti riskien- ja laadunhallintaa osana pilviteknologiaan liittyvien standardien hyödyntämisessä. Tässä diplomityössä on rajattu pois erilaisten palvelutasosopimusten (Service Level Agreement) ja kypsyysmallien näkökulma tietoturvaa ja tietosuojaa edistävänä tekijänä.

1.2 Aikaisempi tutkimus

Tässä työssä keskitytään Järvisen (2003) määritelmän mukaan ”henkilöön tai hänen toimintaansa liittyvien tietojen suojaamista luvatonta keräämistä ja käyttöä vastaan”. Tästä näkökulmasta aikaisempi tutkimus on keskittynyt luotettuun pilvipalvelimien monitorointiin, jolla voidaan auditoida palvelimien toimintoja ja mahdollistaa todistettava näyttö vaatimuksenmukaisuudesta tietoaineiston omistajalle sekä tietoaineiston kuvautuvuuteen, suojautumiseen ja kykyyn luoda turvallinen virtuaalinen ympäristö tietoaineiston käsittelyyn käyttöpoliitikoiden mukaisesti.

1.3 Tutkimuksen menetelmä ja prosessi

Tutkimus on luonteeltaan laadullinen ja teoriaosuus jäsennetty Hirsjärven *et al.* (1997) mukaisen luokittelujen mukaan temaattiseksi. Teoriaosuuden tietieteellinen aineisto on kerätty hyödyntämällä aiheeseen liittyvien tieteellisten artikkeleiden osalta muun muassa Scopusta, ScienceDirectia ja SpringeLinkiä, tietotekniikkaan liittyviä standardeja ja yliopistojen diplomitöitä. Tutkimuskysymyksiin on haettu vastausta kyselytutkimuksella, joka on kohdistettu case-tutkimuksen kohteena oleviin suomalaisiin pilvipalvelun tuottajiin vuonna 2015 sekä analysoitu pilvipalvelujen tuottajien www-sivuilta kerättyä aineistoa. Tutkimuksen kohteena olevia pilvipalvelun tuottajia, heidän palveluja ja tuotteita ei mainita nimeltä anonymiteettisuojan vuoksi.

Tämän työn teoreettisessa osassa luvussa 2 käsitellään pilviteknologiaa ja siihen liittyviä osa-alueita kuten pilviteknologian arkkitehtuuria ja pilvipalvelumalleja sekä pilviteknologiaan liittyviä tiettyjä hyötyjä ja haittoja. Pilviteknologian lisäksi luvussa 3 käsitellään tietoturvaa, tietosuojaa, uhkia ja haavoittuvuuksia. Tietoturvan ja tietosuojan to-

teutuminen edellyttää monien eri asioiden huomioimista; tietoturvauhkien, haavoittuvuuksien ja lainsäädännön merkitys on oleellinen. Luvussa 4 käsitellään pilvipalveluiden tuottamista lähellä olevia standardeja muun muassa tietotekniikkaan ja tietoturvaan liittyviä standardeja. Tämän lisäksi luvussa 4 tarkastellaan tietosuojan näkökulmasta algoritmeja ja niiden nykyistä kehityksen ja tutkimuksen suuntautumista sekä suppeasti laadunhallinnan ja riskienhallinnan eri osa-alueita kuten ulkoistamiseen ja tietojen hajauttamiseen liittyviä riskejä. Luvussa 5 käsitellään pilvipalveluiden tietosuojan varmistamiseen liittyvää tietoaineiston suojausta ja kontrollointia sekä ratkaisuja tietosuojan parantamiseksi erityisesti tietoaineiston suojaamiseksi sitä siirrettäessä ja tallennettaessa pilvipalvelun tallennuslaitteille. Luvussa 6 käsitellään tapaustutkimuksena kolmen eri suomalaisen pilvipalvelun tuottajan tarjoaman pilvipalvelun tietoturvaa tietosuojan näkökulmasta. Luvussa 7 vastataan tämän diplomityön tutkimuskysymyksiin sekä pohditaan suomalaisen pilvipalvelun tuottajan tietosuojaan liittyvien ratkaisujen tietoturvan riittävyyttä yritysten arkaluonteisen tietoaineiston tietosuojan varmistamiseksi.

1.4 Tutkimuksen käsitteet

National Institute of Standards and Technologies (NIST) määrittelee pilvipalvelun seuraavasti, joka on laajasti hyväksytty antaen selkeän kuvan pilviteknologioista ja sen palveluista (NIST 2014):

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud).”

Vapaasti suomennettuna NIST:n edellinen määritelmä: Pilvilaskenta on malli, jolla mahdollistetaan pääsy on-demand itsepalvelusta verkon kautta jaettuun, muokattavissa oleviin tietojenkäsittelyresurssien varastoon (kuten tietoverkkoon, palvelimiin, tietoai-

neisto-varastoihin, sovelluksiin ja palveluihin) joita pystytään nopeasti provosoimaan ja julkistamaan mahdollisimman vähin hallinnollisin vaivoin tai kanssakäymisin palvelun-tarjoajan kanssa. Tämä pilvimalli mainostaa sen saatavuutta ja koostuu viidestä keskei-sestä ominaisuudesta (On-demand itsepalvelu, avoin verkko pääsy, resurssien yhteis-käyttö, nopea joustavuus, palvelun toiminnan mittaus) ja kolmesta palvelumallista (so-vellukset palveluna (SaaS), sovellusalusta palveluna (PaaS), infrastruktuuri palveluna (IaaS), sekä neljästä käyttöönottomallista (yksityinen pilvi, yhteisöllinen pilvi, julkinen pilvi, hybridi pilvi).

2 PILVITEKNOLOGIA

Pilviteknologian juuret johtavat hilalaskentaan, joka alkoi yleistyä 1980-luvun lopulla ja 1990-luvun alussa. Hilalaskennassa jokainen verkkoon liitetty tietokone muodostaa oman solmunsa ja tietokoneiden kokonaisuutta voidaan kuvata ”ritilänä”. Ennen pilviteknologian kehittymistä aina 1990-luvulta lähtien tietotekniikkaa leimasi virtuaalisoinnin käyttöönotto ja kehittyminen. Zhang *et al.* (2010) mukaan 2000-luvulla alettiin ajatella tietojenkäsittelyn ulkoistamista sekä sen myyntiä palveluna kuluttajille ja yrityksille. Armbrust *et al.* (2009) mukaan pilviteknologian kehittymistä ja sen mahdollistamista kaupalliseksi myytäväksi palveluksi voidaan ajatella olevan toisaalta seurasta web-teknologiassa tapahtuvasta nopeasta kehityksestä.

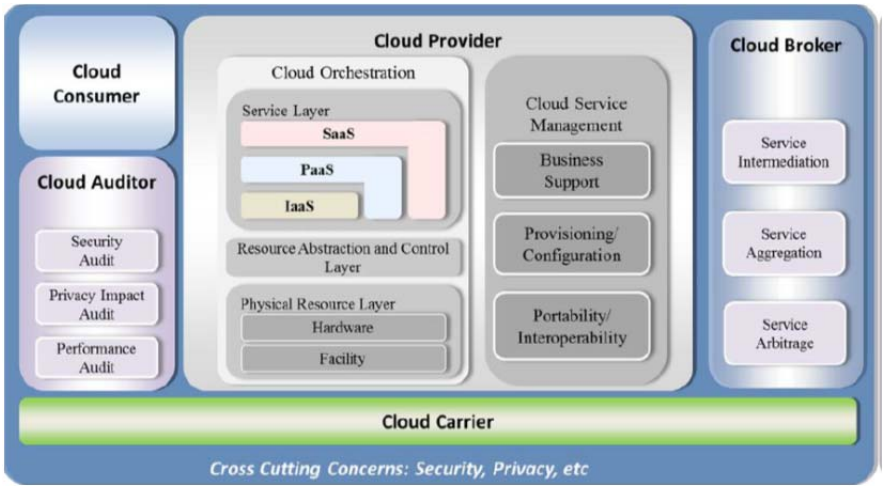
Pilviteknologia haastaa aikaisemman tietojenkäsittelyparadigman, jossa tieto on keskitetty suuriin palvelinsaleihin ja joissa valvonta on 24/7 tuntia vuorokaudessa. Youseffin *et al.* (2008) mukaan tiedon saatavuus on tärkeä tekijä internet palveluja tarjottaessa kuluttajille ja yrityksille pilviteknologiassa; jos yksi pilvi pettää, toinen pilvi pystyy edelleen tarjoamaan pääsyn sovelluksiin ja tietoon. Pilviteknologian avulla verkkopalveluja tarjoavien toimijoiden on mahdollista toteuttaa helposti maailmanlaajuisesti ajasta ja paikasta riippumattomia internet-palveluja.

Youseff *et al.* (2008) mukaan pilviteknologia on herättänyt tutkijoiden mielenkiinnon ja sitä voidaankin pitää edeltäjiensä palvelukeskeisen arkkitehtuurin (Service Oriented Architecture, SOA), hajautettujen järjestelmien ja hilalaskennan sekä virtuaalisoinnin perijänä tutkimuskohteena.

2.1 Pilvirakenteen käsitteellinen malli

Kuvassa 1 on kuvattu pilvirakenteen käsitteellinen malli pilveen integroitujen komponenttien ja prosessien näkökulmasta. Käsitemallissa palvelut on kuvattu organisatorisesta näkökulmasta lähtien. Palvelun tarjoaja (Cloud Provider) mahdollistaa palvelun orkestroinnin, ohjelmisto- ja fyysisen rajapinnan sekä palvelun hallinnan. Palvelun välittäjä (Cloud Broker) huolehtii palvelun tarjoajan ja kuluttajan (Cloud Consumer) välisen

palvelun välitys- ja agregaatiopalveluista. Pilvipalveluiden auditoija (Cloud Auditor) varmistaa kuluttajan puolesta pilvipalvelujen luotettavan, vaatimusten ja käyttöpoliitikoiden mukaisen toiminnan.



***Kuva 1**. Pilvirakenteen käsitteellinen malli (NIST 2014).*

Pilvipalvelun käyttäjä (Cloud Consumer) edustaa henkilöä tai organisaatiota, joka ylläpitää suhdetta ja käyttää pilvipalvelun tuottajan (Cloud Provider) tarjoamaa palvelua. Käyttäjä valitsee pilvipalvelun tuottajan katalogista sopivan palvelun, solmii sopimussuhteen pilvipalvelun tuottajaan ja käyttää palvelua. Riippuen tilatuista palveluista, toiminnoista ja käytöstä voivat palvelut erota pilvipalveluiden käyttäjien joukossa.

Pilvipalveluiden auditoija (Cloud Auditor) arvioi riippumattomasti pilvipalveluja, sovellusten toimintaa, suorituskykyä, tietoturvaa, yksityisyyden suojaa ja liityntää palvelutasosopimuksen parametreihin. Tietoturvatarkastukset ovat hallinnollisia, toiminnollisia, teknisiä varmistuksia tai mittauksia, jotka on otettu sovelluksissa käyttöön suojaamaan luottamuksellisuutta, eheyttä ja saatavuutta ja sen tietoja.

Palvelun välittäjä (Cloud Broker) hallinnoi käyttöä, suorituskykyä ja palveluiden toimitusta sekä neuvottelee asiakassuhteista pilvipalvelun tuottajan ja käyttäjän välillä. Pilvipalveluiden kehittyessä voivat pilvipalveluiden integraatiot tulla liian monimutkaisiksi käyttäjän hallita. Tällaisessa tilanteessa saattaa käyttäjä pyytää pilvipalveluita välittäjältä kuin suoraan niiden tuottajalta. Välittäjä mahdollistaa käyttäjälle yhtenäisen rajapin-

nan useisiin eri pilvipalveluiden tuottajiin, joko liiketoimintaan tai teknisiin tarkoituksiin.

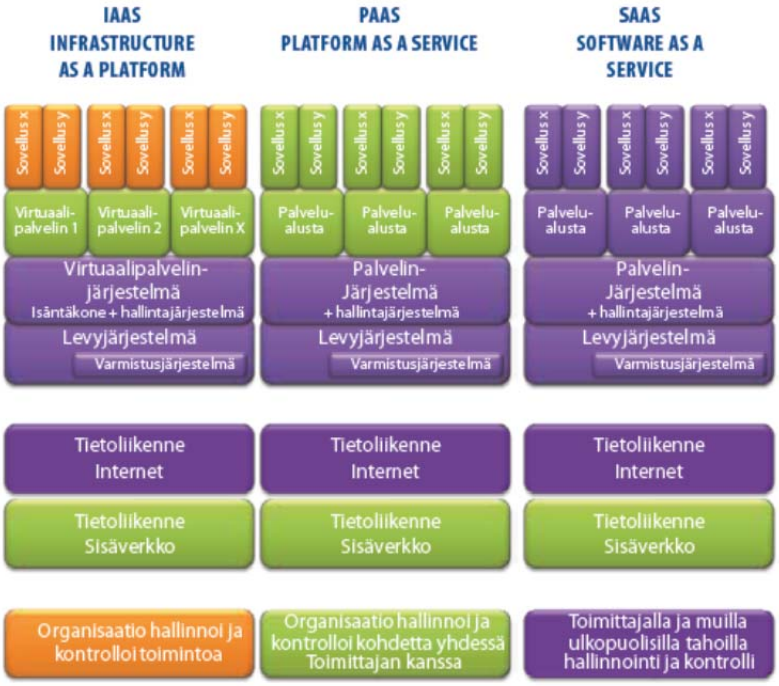
Pilvipalvelun tuottaja (Cloud Provider) voi olla henkilö, organisaatio tai taho, joka mahdollistaa palveluiden saatavuuden käyttäjille. Palvelun tuottaja rakentaa pyydetyt ohjelmisto-, alusta- ja infrastruktuuripalvelut, ylläpitää ja hallinnoi palveluiden tarvitseman teknisen infrastruktuurin, huolehtii palvelutasosopimuksessa sovituista säännöistä, palveluiden tietoturvasta ja yksityisyyden suojasta (NIST 2014).

2.2 Pilviteknologian palvelumallit ja rakenne

Pilvipalvelulla tarkoitetaan Salon (2011) mukaan sitä kokonaisuutta millä pilvipalvelu mahdollistetaan; laitteisto, tietoverkko, datavarasto, palvelut ja käyttöliittymä, joka tuo palvelun asiakkaan käyttöön. Pilvipalveluista puhuttaessa, itse pilvi -käsitteellä tarkoitetaan tietoliikenneverkkoa, jossa ovat nämä palvelun yksityiskohdat piilotettuna.

Pilviteknologian palvelutyypit koostuvat viidestä keskeisestä ominaisuudesta: on-demand itsepalvelu, avoin verkkopääsy, resurssien yhteiskäyttö, nopea joustavuus ja palvelun toiminnan mittaus. Kolmesta palvelumallista: sovellukset palveluna (Software as a Service), sovellusalusta palveluna (Platform as a Service) ja infrastruktuuri palveluna (Infrastructure as a Service). Neljästä käyttöönottomallista, jotka jaetaan yksityiseen pilveen, jossa infrastruktuuri on valjastettu yksinomaan yksittäisen organisaation käyttöön, jonka organisaatio omistaa, hallinnoi ja ylläpitää. Yhteisölliseen pilveen, jossa infrastruktuuria käyttää erityinen kuluttajien, yhteisöjen tai organisaatioiden joukko tai niiden yhdistelmä, joilla on yhteinen agenda. Julkiseen pilveen, joka on avoin kaikille kuluttajille, yrityksille ja yhteisöille. Julkista pilveä hallinnoi ja ylläpitää pilvipalveluiden tuottaja. Hybridi pilveen, joka on edellä mainittujen käyttöönottomallien yhdistelmä.

Yleisimmät pilvipalvelun tuottajan tarjoamat palvelumallit ovat SaaS, PaaS ja IaaS. Katso kuva 2, josta näkee mitä osia eri palvelumalleissa hallinnoi ja kontrolloi organisaatio ja/tai pilvipalvelun tuottaja.



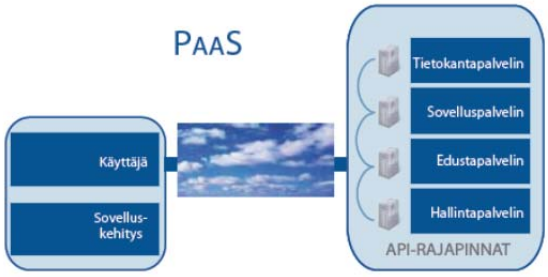
Kuva 2. *Yleisimmät pilvipalvelumallit (VAHTI 2012).*

SaaS-palvelumallissa (katso kuva 3) pilvipalvelun tuottaja ottaa palvelun käyttöön, konfiguroi, ylläpitää ja päivittää sovelluksia käyttäjän kanssa sovitun palvelutasosopimuksen mukaisesti. Palvelun käyttäjä/organisaatio ostaa yleensä valmiin palvelun, jolloin palveluntarjoaja voi toteuttaa palvelun millä tahansa haluamallaan teknisellä ratkaisulla, kunhan se täyttää palvelusopimuksen vaatimukset (VAHTI 2012). Käyttäjällä on rajoitetut ylläpito-oikeudet sovellukseen. Käyttäjä saa palvelut käyttöön web-käyttöliittymän tai asiakassovelluksen avulla. Esimerkkejä SaaS-palveluista ovat sähköpostipalvelu, SSL-VPN-palvelu tai tietoturvapalveluja kuten virustentorjunta.

Kuva 3. *SaaS-palvelussa organisaatio ostaa valmiin palvelun, jota toimittaja tuottaa asiakkaalle sopimuksessa määritettyjen ehtojen mukaisesti (VAHTI 2012).*

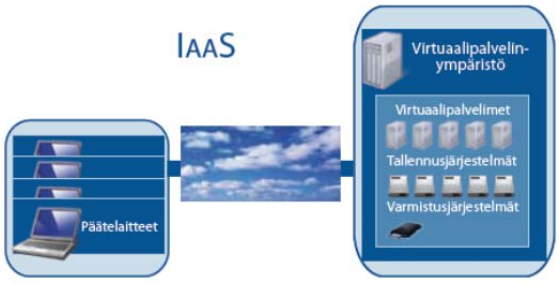
PaaS-palvelumallissa (katso kuva 4) pilvipalvelun tuottaja hallinnoi alustan infrastruktuuria, sopimusehtoja ja resursseja mahdollistaen käyttäjälle kehitystyökalut, testauksen,

käyttöönoton ja sovellusten hallinnoinnin. Käyttäjällä ei ole kuitenkaan hallinnointioikeuksia fyysiseen infrastruktuuriin kuten verkkoon, palvelimiin, käyttöjärjestelmiin tai levymuisteihin. Esimerkkejä PaaS-palveluista ovat Microsoft Azure tai Google App Engine.



Kuva 4. *PaaS-palvelussa organisaatio voi ostaa täydellisen sovelluskehitys- ja tuotantoympäristön uuden palvelun kehittämiseksi ja tuottamiseksi (VAHTI 2012).*

IaaS-palvelumallissa (katso kuva 5) palvelun tuottaja huolehtii palvelun fyysisestä suorituskyvystä, palvelimista, verkosta, muisteista ja muista laiteresursseista. Pilvipalveluiden käyttäjä voi hallinnoida fyysisen infrastruktuurin päällä olevaa virtuaaliympäristöä kuten ottaa käyttöön sovelluksia ja ajaa niitä. Esimerkkejä IaaS-palveluista ovat Amazon EC2 tai VMware vCloud (NIST 2014).

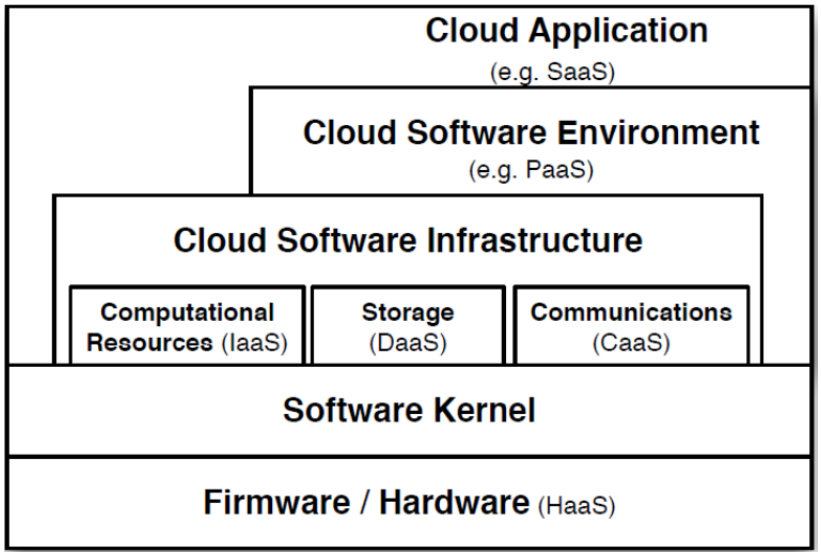


Kuva 5. *IaaS-palvelua ostaessaan organisaatio ulkoistaa palvelutoimittajalle kaikki tai osan omassa hallinnassaan ja omistuksessaan olleesta teknologiasta. Kuvasta puuttuvat tietoliikenneyhteyden suojaukseen tarvittavat palomuuri- ja muut ratkaisut (VAHTI 2012).*

Vaquero *et al.* (2009) mukaan pilvipalvelun rakennetta voidaan kuvata myös eri toimijoiden ja kerrosten välisenä kokonaisuutena. Youseff *et al.* (2008) jakavat pilviteknologian viiteen eri tasoon, joita ovat (kuva 6):

- sovelluskerros

- ohjelmistoympäristöt
- ohjelmistoinfrastruktuuri
- ohjelmistoydin
- laitteisto



Kuva 6. *Pilvipalvelun eri tasot (Youseff et al. 2008).*

Youseff *et al.* (2008) mukaan sovelluskerroksen ollessa pilvipalvelun käyttäjälle näkyvin osa-alue, on se myös hyvä esimerkki pilven hyödyistä tietojenkäsittelyn siirtyessä pois työasemalta laitteistotason palvelimille. Vaqueron *et al.* (2009) mukaan esimerkkinä sovelluskerroksen ohjelmistoista voidaan pitää muun muassa tekstinkäsittelysovelluksia. Sovellustason palvelu on nimeltään palveluohjelmisto (Software as a Service, SaaS).

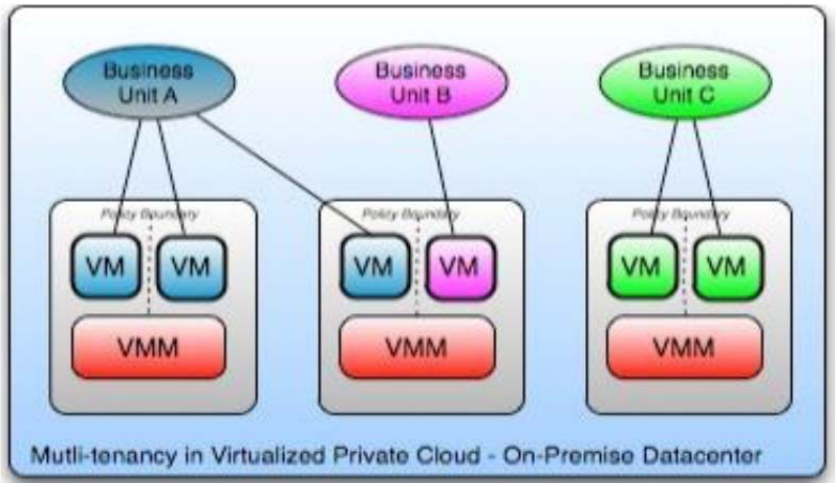
Toisena kerroksena mallissa on ohjelmistoympäristö. Ohjelmistoympäristöä hyödyntävät sovelluskehittäjät, joille kerros tarjoaa ohjelmointi- ja ympäristörajapinnan. Youseff *et al.* (2008) mukaan ohjelmistoympäristön avulla pilven ympäristöjen kanssakäymistä saadaan kehitettyä ja pilven skaalatutuvuutta parannettua. Vaquero *et al.* (2009) mukaan ohjelmistoympäristö tarjoaa ohjelmistoalustan, jossa tietojärjestelmiä voidaan ajaa. Vaquero *et al.* (2009) mukaan palveluna tarjottavaa ohjelmistoympäristöä kutsutaan yleisesti pilvialustaksi (Platform as a Service, PaaS).

Kolmantena kerroksena mallissa on ohjelmistoinfrastruktuurin kerros, joka on perustavanlaatuinen kahdelle ylimmälle kerrokselle, mutta se voidaan myös ohittaa sovelluksia tai ohjelmistoympäristöä suunniteltaessa. Ohjelmistoinfrastruktuurikerros on jaettavissa vielä kolmeen alakategoriaan: laskennallisiin resursseihin, tiedon tallentamiseen ja tiedonvälitykseen. Laskennalliset resurssit pitävät pääosin sisällään virtuaalisoinnin, tiedon tallentamiseen taas liittyy tiedon replikointi sekä hajauttaminen. Youseff *et al.* (2008) mukaan tiedonvälitys on elintärkeä osa-alue pilviteknologian palvelun laadun kannalta. Ohjelmistoinfrastruktuuri voidaan samalla tapaa kuin muut kerrokset tarjota palveluna, jolloin asiakasorganisaatiolle, tässä tilanteessa palveluntarjoajille, voidaan rakentaa tilapäistarpeen täyttäviä järjestelmiä. Vaquero *et al.* (2009) mukaan ohjelmistoinfrastruktuuripalvelua voidaan kutsua yksinkertaisesti palveluinfrastruktuuriksi (Infrastructure as a Service, IaaS).

Mallin neljännessä kerroksessa on ohjelmistoydin. Ohjelmistoytimen tehtävänä on toimia väliohjelmistona, joka hallitsee fyysisien palvelimien ohjelmistoja. Ontologian viidentenä ja alimmaisena kerroksena toimii laitteistokerros, joka on myös pilviteknologian selkäranka.

2.3 Pilvipalveluiden arkkitehtuuri

Pilviteknologian palvelutyyppien arkkitehtuuri perustuu multitenantti-arkkitehtuuriin (multitenant = monta vuokralaista), jossa yhtä sovellusinstanssia käyttävät kaikki palvelun käyttäjät siten, että asiakaskohtaiset tiedot on eristetty toisistaan (Kuva 7). Aikaisemmin arkkitehtuuri perustui singletenant-arkkitehtuuriin, jossa jokaiselle asiakkaalle asennettiin omaan palvelinkoneeseen instanssi sovelluksesta sekä tietokannasta. Ratkaisun hyvänä puolena oli räätälöitävyys mutta heikensi huomattavasti ylläpidettävyyttä.



Kuva 7. *Asiakaskohtaiset tiedot on eristetty toisistaan (CSA 2014).*

Multitenantti-arkkitehtuurissa sama sovellusinstanssi palvelee kaikkia käyttäjiä, jossa myös muutokset sovelluksessa ovat kaikilla palvelun käyttäjillä samanaikaisesti käytettävissä. Myös tietokanta jaetaan multitenantti-arkkitehtuurissa. Tällöin on tärkeää tietoturvasyistä erottaa eri asiakkaiden tietoaineisto toisistaan. Yleisesti käytetään tietokantaskeemoja, joiden avulla voidaan yhden tietokannan sisälle luoda jokaiselle asiakkaalle oma suojattu alue (Somea ICT Solutions 2014).

Multitenantti-arkkitehtuurit perustuvat web-arkkitehtuuriin. Yleensä SaaS-palvelumallin tuotteet rakennetaan web-ympäristöön, joten web-alustojen erityisosaaminen on tärkeää SaaS-tuotekehityksessä. Web-ohjelmistojen tuotekehityksessä suurimpia haasteita ovat teknologioiden ja alustojen monimuotoisuus, jossa alusta tulisi osata valita suunniteltavan järjestelmän mukaan. Teknologian valitaan ei ole mitään yleispätevää ratkaisua, vaan asiaa tulee tarkastella ja testata aloitettaessa kehitystyötä. Teknologioiden monimuotoisuus on johtanut myös siihen, että sovellusten ohjelmoinnissa hyödynnetään useita ohjelmointi-, skripti- ja kuvauskieliä. Tämä asettaa tiettyjä osaamisvaatimuksia kehityshenkilöstön ja -ympäristön hallinnan suhteen (Somea ICT Solutions 2014).

Pilvipalveluiden kehittäminen on luonteeltaan asiakas-palvelinpohjaista, jossa osa toiminnoista suoritetaan käyttäjien selaimissa ja osa palvelun tuottajan palvelimilla. Palvelinohjelmisto jakautuu usein tilattomaan liiketoimintalogiikkaan sekä pysyvään tietoaineistovarastoon, esimerkiksi tietokantaan. Rich client -tekniikoiden kehitys on viime aikoina mahdollistanut laskentakuorman siirtämisen entistä enemmän palvelimelta asi-

akkaan selaimeen. Web-kehityksessä merkitsee myös osittain sovelluksen toimivuus eri selaimissa, mutta tämä ei ole yhtä hankala haaste kuin esimerkiksi mobiilikehityksessä (Somea ICT Solutions 2014).

Monissa SaaS-palvelumalleissa ohjelmistoa kehitetään jatkuvasti ja uusia versioita julkaistaan tiheällä syklillä. Multitenanti-arkkitehtuurissa perinteinen ohjelmistojen versiointi-ajattelu on hämärtynyt, koska usein SaaS-palvelumallissa ohjelmistosta on olemassa vain yksi kaikille käyttäjille yhteinen versio. Tämä malli mahdollistaa nopeammin reagoimaan käyttäjien muuttuneisiin tarpeisiin sekä myös markkinoiden muutoksiin, mikä toisaalta tekee tuotekehityksestä entistäkin nopeatahtisempaa (Somea ICT Solutions 2014). Web-sovellusten tietoturvan parantamiseksi suosittelee Cloud Security Alliance noudattamaan esimerkiksi The Open Web Application Security Projectissa (OWASP) esitettyjä hyviä käytäntöjä.

2.4 Pilviteknologian hyödyt ja ongelmat

Jensen *et al.* (2009) mukaan pilvipalveluiden avulla saavutettavana hyötynä voidaan pitää pääomamenojen ja operatiivisten kulujen vähenemistä. Armbrustin *et al.* (2009) mukaan säästöjä syntyy kiinteiden kulujen siirtyessä muuttuviin kuluihin. Tästä syystä pilvipalvelujen ja siihen liittyvien tuotteiden käyttöönotto ja kehittäminen eivät vaadi yhtä suurta riskinottoa kuin aikaisemmin. Myös palvelujen keskittäminen pilveen hyödyntää Armbrust et *al.* (2009) mukaan kuluttajia ja palveluita hyödyntäviä yrityksiä koska palveluntarjoajat tekevät ohjelmistoasennukset, korjaukset ja päivitykset. Youseff *et al.* (2008) pitävät tämänkaltaista ratkaisua toimivana myös sovelluskehittäjien kannalta. Sovelluskehittäjät voivat tehdä korjauspäivityksiä ohjelmistoihin tai päivittää uusia ominaisuuksia ilman, että loppukäyttäjien työ siitä vaikeutuu. Pilvestä ajettavien sovellusten etuna on myös, että se vähentää tarvetta hankkia loppukäyttäjille prosessointi- tai muistikapasiteetiltaan tehokkaita työasemia.

Pilviteknologian etuna on myös sen käytettävyys. Pilvipalveluiden kapasiteettiresursseja voidaan hallita ohjelmistollisesti, mikä auttaa palvelun tilaajaa keskittymään omaan liiketoimintaan vähentäen tietojenkäsittelyresursseja ja yksityiskohtien syvällistä osaamista sekä hallintaa. Vaqueron *et al.* (2009) mukaan juuri pilvipalveluiden käytettävyys on

yksi merkittävimmistä tekijöistä, jotka edistävät sen omaksumista ja käyttöönottoa. Pilvipalveluita käyttävä asiakas maksaa ainoastaan tietojenkäsittelyyn käyttämästään ajasta. Yritysten tietojenkäsittelyyn tarvitsemat resurssit ovat normaalisti huomattavasti pienemmät kuin ruuhka-aikoina. Youseff *et al.* (2008) mukaan ylimitoitetut resurssit ovat yrityksille tästä syystä huomattava kustannustekijä. Armbrust *et al.* (2009) mukaan taas pilvipalveluiden käyttäminen mahdollistavat tehokkaan tavan ottaa huomioon väliaikaiset, tavallisesta poikkeavat resurssitarpeet, jossa palvelun käyttäjä maksaa ainoastaan käyttämästään ajasta. Resurssitarpeen yli- tai aliarviointi ei aiheuta tästä syystä merkittäviä käyttökustannuksia.

Tietotekniikkapalveluiden ollessa tärkeä osa liiketoimintaa, sovitaan palveluehdoista yleensä palvelutasosopimuksissa (Service Level Agreement, SLA). Greenin (2007) mukaan palvelutasosopimukset ovat muodostuneet välttämättömiksi de facto -sopimuksiksi erityisesti informaatioteknologiaan liittyvillä aloilla, joissa erilaiset ulkoistamiset ovat yleisiä.

Youseff *et al.* (2008) mukaan turvallisuuteen ja tietosuojaan liittyvät osa-alueet ovat merkittävimpiä pilviteknologian laajempaa käyttöä hidastavia tekijöitä. Standardoinnissa olevien puutteiden vuoksi tietoturva, tiedon yksityisyys ja omistukseen liittyvät asiat ovat jokaisen pilvipalveluita tarjoavan tahon itse määrittelemiä. Jensenin *et al.* (2009) mukaan yrityksen tietojen sekä sovellusten asettaminen täysin ulkopuolisen tahon varaan, joka voi olla toisella puolella maailmaa valtiossa, jossa on erilaiset säännökset, saattaa aiheuttaa halun pitäytyä perinteisemmissä tietojenkäsittelytavoissa.

Zhang *et al.* (2010) mukaan tietotekniikkapalvelujen ostaminen edullisesti saattaa synnyttää halukkuutta aloittaa monta projektia liian nopealla tahdilla. Myös Zhang *et al.* (2010) mukaan tietotekniikan ulkoistamista tulisi harkita tilannekohtaisesti. Pilvipalvelu voi antaa ratkaisun joihinkin ongelmiin, mutta saattaa toisaalta aiheuttaa entistä haastavampia ongelmia. Subashini *et al.* (2011) mukaan erityinen ongelma liittyen vakioituun palvelutasoon pilvipalveluissa on juuri tietoturvaosa-alueiden, kuten palomuurien ja kuormantasauksen, alkeellinen taso.

Armbrust *et al.* (2009) mukaan merkittävä ongelma on myös pilvipalveluiden saatavuus. Liiketoiminnan ollessa vahvasti sidoksissa ulkoistettuihin pilvipalveluihin eivät yritykset ole halukkaita ostamaan palveluita, jos palveluja tarjoavalla organisaatiolla ei ole strategiaa palvelun tarjonnan keskeytyessä äkillisesti. Rimal *et al.* (2009) mukaan siirrettäessä tietotietotekniikkapalveluja pois yrityksen omista käsistä, kohdistuu ongelmatilanteissa liiketoimintaan vakava uhka. Luotettavuus on koetuksella, kun aika on rahaa. Jotta useiden pilvien välinen saatavuus ja toiminnallisuus voidaan taata, tulee myös pilvien kehittämisessä ottaa huomioon yhtyeenliitettävyys.

2.5 Yhteenveto

Pilvipalvelut perustuvat nykyisin multitenanti-arkkitehtuuriin, jossa on mahdollista käyttää yhtä sovellusinstanssia käyttäjien tietoaineiston erottamiseksi toisistaan hyödyntämällä tietokantaskeemoja, joiden avulla virtuaalipalvelimelle voidaan perustaa omia suojattuja alueita.

Yleisempiä pilvipalvelumalleja ovat IaaS, SaaS ja PaaS. Pilvipalvelumalleista SaaS-palveluja käyttävät organisaatiot tai kuluttajat esimerkiksi sähköposti- ja toimisto-ohjelmistopalveluja. Yritykset käyttävät yleensä liiketoiminnan tehostamiseksi IaaS-palveluja siirrettäessä infrastruktuuri-palveluja pilveen kustannusten säästämiseksi.

Tietojenkäsittelyinfrastruktuurin ulkoistaminen pilveen tuo yrityksille merkittäviä säästöjä pääoma- ja operatiivisten menojen laskiessa kun ei tarvitse investoida kalliiseen infrastruktuuriin ja henkilöstöön, joka ylläpitää tietotekniikkapalveluja. Kuitenkin pilvipalveluiden käyttöönottoa ja liiketoiminnan siirtämistä pilveen hidastaa epävarmuus tietoturvan ja tietosuojan riittävästä tasosta suojata arkaluontoista tietoaineistoa pilvessä. Ongelmana ovat myös standardoinin puutteet liittyen tietoturvaan, tiedon yksityisyyteen ja omistajuuteen.

3 PILVITEKNOLOGIAN TIETOTURVA JA TIETOSUOJA

Pilvilaskenta on viime vuosina kasvanut merkittäväksi liiketoiminnaksi tietotekniikkateollisuudessa, joka mahdollistaa kasvattamaan tietojenkäsittelykapasiteettia sekä lisäämään dynaamisesti tietotekniikan mahdollisuuksia investoimatta uuteen infrastruktuuriin, kouluttamalla uutta henkilökuntaa tai hankkimalla kalliita ohjelmistolisenssejä. Pilvipalveluiden käytön ja pilveen tallennetun tietoaineistomäärän kasvaessa, on kuluttajien ja yritysten keskuudessa kasvanut myös huoli sen tietototurvallisuudesta. IDC tutkimuksen mukaan pilvipalvelujen myynti oli vuonna 2010 21,5 miljardia dollaria ja vuonna 2015 sen ennustetaan kasvavan jo 72,9 miljardiin dollariin (IDC 2014).

Tilastokeskuksen marraskuussa 2014 julkaiseman ”Tietotekniikka yrityksissä” tutkimuksen mukaan maksullisia pilvipalveluja käyttää suomalaisista yrityksistä 51%. Yleisemmin pilvipalveluna käytetään sähköpostia 33 % ja tallennuspalveluja 27 % yrityksistä. Suurin este siirtyä käyttämään pilvipalveluita on tiedon puute 42 % ja tietoturvariskit ja epävarmuus tietojen sijainnista pilvipalvelussa 28 % osuus yrityksistä, jotka eivät ole ottaneet pilvipalveluja käyttöön (Tilastokeskus 2015).

Pilvipalveluita käytetään Suomessa lähinnä sähköposti, tiedostojen tallennus ja muina vastaavina Software as a Service-palveluina. Subashini *et al.* (2011) mukaan pilvipalveluiden tietoturvallisuus liittyen tiedon suojaamisen ja yksityisyyden suojaan, ovat merkittävimpiä tekijöitä alentamaan pilvipalvelujen laajempaa käyttöönottoa.

Pilvipalveluja tuotettaessa on tärkeää tietosuojan näkökulmasta huomioida myös tietosuojalainsäädäntöön liittyvät asetukset suojattaessa kuluttajan yksityisyyttä sen käytäessä pilvipalveluja. Seuraavissa luvuissa käsitellään lyhyesti pilvipalvelujen tietoturvaa, tietosuojaa ja tietoturvauhkia.

3.1 Pilviteknologian palvelumallien tietoturva

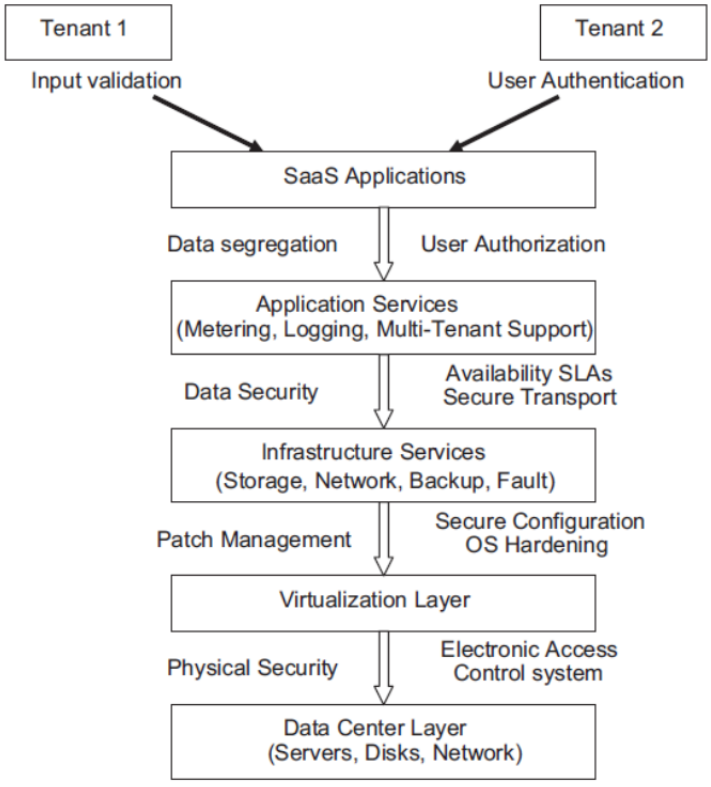
Pilvipalveluiden tietoturvan näkökulmasta luotettavuus ja käytettävyys liittyvät keskeisesti pilviteknologian ja pilvipalveluiden tietoturvaan. Luotettavuuden merkitystä voidaan perustella pilviteknologialle luonteenomaisella palvelurakenteella ja tähän liittyvällä tietojenkäsittelyn ulkoistamisella. Vaqueron *et al.* (2009) mukaan käytettävyys on keskeinen pilviteknologian nopeaan yleistymiseen vaikuttava tekijä.

IaaS-, PaaS- ja SaaS-palvelumallit mahdollistavat infrastruktuuriresurssit, sovellusalustan ja ohjelmistopalvelut kuluttajille ja yrityksille. Nämä palvelumallit sisältävät eritasoisia tietoturvavaatimuksia pilviympäristön teknologian luotettavuudelle ja käytettävyydelle. IaaS-palvelumalli luo perustan kaikille pilvipalveluille, jonka päälle on rakennettu PaaS- ja SaaS-palvelut (kuva 1, sivulla 7). Subashini *et al.* (2011) mukaan näiden palvelujen ominaisuudet ovat periytyviä ja siten informaation tietoturva ja riskit periytyvät palvelutyyppien välillä. Seuraavassa on kuvattu erityisesti SaaS-palvelumallin tietoturvaa koska suurin osa kuluttajista ja organisaatioista käyttävät näitä palveluja.

SaaS-palvelumallissa toimittajat tarjoavat asiakkailleen merkittäviä hyötyjä kuten toiminnallista tehokkuutta ja alempia kustannuksia. SaaS-pilvipalvelumallissa toimittajat saattavat laajentaa omaa toimintaansa replikoimalla kuluttajien ja yritysten tietoaineiston maailmanlaajuisesti varmistaakseen näin korkean käytettävyyden ja palvelujen saatavuuden. Pilvipalveluiden tuottajat saattavat myös ulkoistaa ylläpidon kolmansille osapuolille kuten on tehnyt esimerkiksi Amazon ja Google (Subashini *et al.* 2011). Tästä syystä pilvipalveluiden käyttäjien on vaikea kontrolloida ja varmistua tietoturvan riittävästä tasosta ja palvelun luotettavuudesta ja saatavuudesta.

Subashini *et al.* (2011) mukaan pilvipalveluiden käyttäjillä erityisesti yrityksillä on suuri huoli tietovuodoista, sovellusten haavoittuvuuksista, luotettavuudesta ja saatavuudesta, joka voi johtaa taloudellisiin menetyksiin ja juridisiin ongelmiin. Tästä syystä palveluntarjoajat pyrkivät parantamaan tietoturvaansa ja kohentamaan sen kautta imagoansa esimerkiksi Google on läpäissyt SAS70 type-II-auditoinnin ja näin parantanut kuvaa kuluttajille tietoturvatasostaan (Salo 2011).

Kuvassa 8 on kuvattu miten tavallisesti pilvipalveluiden toimittajat varmistavat tietoturvan SaaS-pilvipalvelumallin eri tasoilla. SaaS-palvelumallissa toimittajat ovat pakotettuja rakentamaan lisäturvaa varmistaakseen palvelun tietoturvan muun muassa ehkäisemällä tietovuodot, jotka johtuvat tietoturva-aukoista sovelluksissa tai pahantahtoisista toimittajan työntekijöistä. Väärinkäytösten ehkäisemiseksi, edellyttää tämä pilvipalveluiden tuottajia käyttämään vahvan salauksen tekniikoita kuten Secure Socket Layer (SSL) niin pääsynvalvonnassa kuin tietoaineiston suojaamisessa. Myös pilvipalveluiden tuottajien tulee tarkastella kuvan 8 tietoturva-elementtejä huolellisesti osana SaaS-sovellusten kehitystä ja ylläpitoa.



***Kuva 8**. SaaS-palvelumallin tietoturvatasot (Subashini et al. 2011).*

Kuvassa 8 esitettyjä tärkeimpiä tietoturva-elementtejä ovat tietoaineiston eheyteen ja luottamuksellisuuteen liittyvät tietoturva-tasot kuten käyttäjän autentikointi ja käyttöoikeuksien rajaaminen palvelussa, asiakkaiden tietoaineiston eriyttäminen palvelussa, tietoaineiston käsittelyyn liittyvät tietoturvaratkaisut, joilla varmistetaan tietoaineiston eheys ja luottamuksellisuus, infrastruktuurin verkon tietoturvaratkaisut ja ylipäätänsä palvelun saatavuus sekä virtuaalipalvelimien että fyysisen tason suojaus.

Esimerkiksi Suomen valtion viranomaista edellytetään noudattamaan tietoaineiston turvaamisessa kansallista turvallisuusauditointikriteeristöä (KATAKRI 2011).

Kriteeristö on jaettu neljään pääosioon:

- hallinnollinen turvallisuus (turvallisuusjohtaminen)
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoturvallisuus

Jokaiselle edellä mainituista osioista on laadittu yksityiskohtiin menevä kolmiportainen vaatimusluokittelu, joka noudattaa valtionhallinnon tietoturvallisuuden tasokäsitteitä – perustaso, korotettu taso ja korkea taso. Esimerkiksi, jos tietoaineisto luokitellaan kuuluvaksi ST III suojaustasoon, edellytetään pilvipalvelulta korkeampaa tietoturva-tasoa kuin mitä tarjoaa esimerkiksi julkisen pilven käyttöönottomalli tietoaineiston suojaamiseksi.

3.2 Pilvipalveluiden tiedon eheys ja luottamuksellisuus

Tiedon eheys ja luottamuksellisuus hajautetuissa pilvipalveluissa on eräs tärkeimmistä kysymyksistä niin kuluttajille kuin yrityksille. Subsihinin *et al.* (2011) mukaan tiedon eheydessä ja luottamuksellisuudessa nousevat esiin muun muassa seuraavia kysymyksiä:

- Yksityisyydensuoja- ja luottamuksellisuusriskit vaihtelevat merkittävästi pilvipalvelun toimittajan mukaan
- Tiedon tyypin ja pilvikäyttäjän luokituksen mukaan yksityisyys ja luottamuksellisuus vaihtelevat kun tieto julkaistaan pilvipalvelussa
- Tiedon sijainnilla pilvipalvelussa saattaa olla merkittävä vaikutus tiedon yksityisyyden suojaan ja luottamuksellisuuteen koska sama tieto saattaa sijaita useassa paikassa samaan aikaan
- Eri maiden lait voivat mahdollistaa pilvipalvelun toimittajan tutkimaan palveluun tallennettuja tietoja rikollisuuden estämiseksi

- Eri maiden lait tekevät vaikeaksi arvioida tietoa pilvipalvelussa samoin kuin yksityisyyden ja luottamuksellisuuden suojaa

Subsihini *et al.* (2011) mukaan tiedon eheyden varmistaminen sovelluksissa, jotka käyttävät ainoastaan yhtä tietokannanhallinta-järjestelmää, voidaan tiedon eheys kannassa varmistaa ACID-ominaisuudella (Atomicity, Consistency, Isolation, Durability). Pilvipalvelut ovat taas hajautettuja järjestelmiä, joissa käytetään useita tietokantojen hallinta-järjestelmiä ja sovelluksia. Tästä syystä tiedon eheyden varmistamiseksi, tulee pilvipalvelun tukea keskitettyä globaalista tapahtumienhallintaa. ACID käsite on kuvattu ISO/IEC 10026-1:1992 luvussa 4 (ISO 2015). Yleisesti tapahtumienhallinta tai monitorointi on suunniteltu ymmärtämään ACID käsitettä.

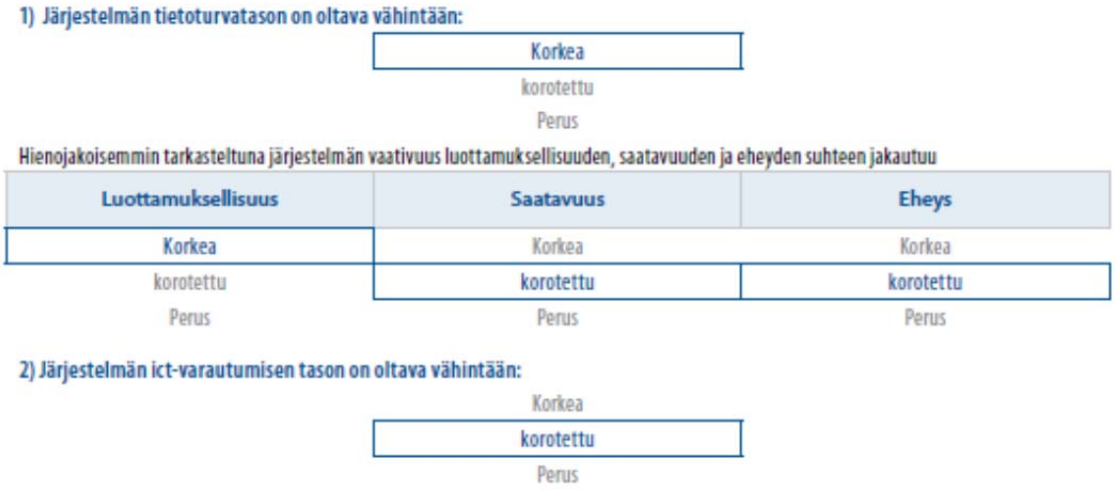
SaaS-palveluiden toimittajilla on kuitenkin ollut suuria haasteita verkkopalveluiden tapahtumien hallinnassa koska http-protokolla ei tue tapahtumia tai takaa luettavaa tietoaineiston toimittamista. Ainut mahdollisuus on ollut toteuttaa tämä verkkosovelluksen API (Application Program Interface) -rajapinnassa.

3.3 Tietosuojaan liittyvä lainsäädäntö ja vaatimuksenmukaisuus

Suomessa toimivan pilvipalvelun tuottajan tulee huomioida erialaisia tietosuojaan liittyviä lakeja ja tietoturva-ohjeita tuotettaessa palveluja yksityisyyden suojan säilyttämiseksi pilvessä. Tietosuojaan liittyviä lakeja Suomessa ovat muun muassa:

- Henkilötietolaki (523/1999)
- Laki verotustietojen julkisuudesta ja salassapidosta (1346/1999)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Sähköisen viestinnän tietosuojalaki (516/2004)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Luottotietolaki (527/2007)

Valtiovarainministeriön VAHTI 3/2012 teknisen ICT-ympäristö tietoturvataso-ohjeessa on kuvattu eri ICT-ympäristöissä tietoaineistojen suojaaminen perustuen kansalliseen turvallisuusauditointikriteeristö KATAKRI-ohjeistukseen tietoturvatasoista. Kuvassa 9 on esitetty järjestelmän tietoturvataso sekä ICT-varautumisen taso silloin kun käsitellään ST III luokiteltua tietoaineistoa, joka on KATAKRIssa luokiteltu korotetulle tasolle.



Kuva 9. *Teknisen ympäristön vaatimukset tietoaineistolle, joka on luokiteltu korotetulle tasolle (VAHTI 2012).*

3.4 Tietoturvauhat ja haavoittuvuudet

Kellermanin (2010) mukaan pilviteknologian hyödyntämiseen liittyy useita erilaisia tietoturvauhkia. Kuluttajilla ja yrityksillä on liiallista luottamusta palvelun tuottajan kryptausmenetelmiin ja palvelun infrastruktuurin tietoturvaan. Pilvipalveluiden tietoturvaa ovat krakkerit pyrkineet murtamaan esimerkiksi internet-selaimista löytyneiden haavoittuvuuksien kautta. Hyökkääjä on voinut myös hyödyttää niin kutsua wrapping-tekniikkaa, jossa tiedoston otsaketietoja on muokattu mahdollistaen näin suorittamaan laittomia komentoja kohdetietokoneella. Hyökkäys voi kohdistua myös pilven infrastruktuuriin. Jensenin *et al.* (2009) mukaan hyökkäys on voitu kohdistaa pilven infrastruktuuriin soluttamalla haittaohjelmia, vahingollinen palvelumoduuli tai virtuaalikone osaksi pilvikokonaisuutta ja näin vakoilla tietoliikennettä. Pilvipalvelun saatavuutta voidaan haitata myös palveluestohyökkäyksillä. Modi *et al*. (2013) esittää, että pilven valtuutetut käyttäjät ovat huolissaan sisäisestä uhkasta, jossa käyttäjät yrittävät saada

valtuuttamattomat oikeudet tai väärin käyttävät valtuutettuja oikeuksia tehdäkseen petoksen, paljastaen tietoja toisille tai vahingoittaen tai tuhoten tietoja. Modi *et al.* (2013) mukaan tämä voi muodostaa vakavan luottamus kysymyksen pilvipalvelun tuottajien ja käyttäjien välille.

SaaS-palveluiden tietoturvan kehittämisessä tulee kiinnittää erityistä huomioita tietoaineiston suojaamiseen, verkon suojaamiseen, pääsynvalvontaan ja verkkosovellusten ja virtuaalisoinnin haavoittuvuuksiin tiedon eheyden, luottamuksellisuuden ja saatavuuden varmistamiseksi. Subashini *et al.* (2011) mukaan SaaS-pilvipalvelun tietoturvan heikkouksia testataan ja validoidaan ainakin seuraavia tietoturvauhkia vastaan:

- Pääsynvalvonta
- Verkkohyökkäykset (cross-site scripting)
- Käyttöjärjestelmä- ja tietokantavuodot (OS ja SQL injection)
- Verkkoväärennös pyynnöt (cross-site request forgery)
- Manipulointi (cookie ja hidden field manipulation)
- Tiedontallennusvälineet ja konfiguraatiot

Subashini *et al.* (2011) mukaan tietoturvauhka liittyy aina jossain määrin tiedon altistumiseen taholle, jonka ei tulisi päästä tietoon käsiksi. Näin ollen tietoturva integroituu olennaisesti osaksi tiesuosuojaa. Esimerkiksi Amazon on parantanut pilvipalvelun tietoliikenneverkon tietosuojaa, jolla on voitu vähentää merkittävästi mies välissä hyökkäyksiä (man-in-the-middle-attack), ip-huijauksia, portin skannaamista, ip-pakettien nuuskimista ja niin edelleen.

Pilvipalveluihin liittyy seuraavia mahdollisia tietoturvahaasteita ja -uhkia (NIST 2014):

- Tiedon luottamuksellisuus ja eheys siirrettäessä tietoaineistoa pilveen ja pilvestä
- Hyökkäykset, jotka käyttävät hyväksi pilven yhtenäisyyttä ja pilvilaskentajärjestelmän heikkouksia ja laskentatehoa
- Kelvoton pilvipalvelun todentaminen ja valtuuttaminen mahdollistaa pääsyn ohjelmistoihin, tietoihin ja resursseihin toisen valtuutetun käyttäjän oikeuksilla

- Heikosti suunnitellut ja ohjelmoidut internet-pohjaiset sovellukset ja haavoittuvuudet yksityisissä verkoissa mahdollistavat hyökkäyksen pilvipalveluihin
- Pilvipalvelun tietoaineiston salauksen puutteet
- Pilvipalvelun saatavuusrajoitteet, jotka johtuvat pilvipalveluiden epästandardeista ohjelmarajapinnoista siirryttäessä toiseen pilveen
- Hyökkäykset, jotka hyödyntävät virtuaalikoneiden tunnettuja haavoittuvuuksia
- Hyökkäykset, jotka hyödyntävät globaalien politikoiden ja sääntöjen epäyhtenäisyyttä
- Hyökkäykset, jotka hyödyntävät toimitusketjun haavoittuvuuksia kun pilvipalvelun toimittaja siirtää komponentteja palveluntuottajalle
- Tietoaineiston salakuuntelu siirron aikana

3.5 Yhteenveto

Siirrettäessä tietoaineistoa pilveen siirretään samalla myös suurimmaksi osaksi kontrolli pois pilvipalvelua käyttävältä asiakkaalta pilvipalvelua tarjoavan organisaation hallintaan.

Tietosuojan näkökulmasta tulee tällöin varmistua erityisesti palvelun tarjoajan tietoturvasta koskien käyttäjän autentikaatiota, käyttöoikeuksien rajaamista ja tietoaineiston eriyttämisestä pilvessä sekä miten tietoaineistojen käsittelyyn liittyvät tietoturvaratkaisut on toteutettu palvelussa. Tärkeää on myös varmistua, että tietoaineisto ei siirry toiseen maahan, jossa on erilainen lainsäädäntö koskien tietosuojaa ja yksityisyyttä.

4 PILVITEKNOLOGIAN KEHITTÄMINEN

Eräs tapa kehittää saatavuutta ja toiminnallisuutta on standardointi. Pilviteknologian kehittymisen edellytyksenä on Kaufmanin (2009) mukaan ennakoiva toiminta, esimerkiksi standardoinnin avulla. Hilalaskennasta perityistä, standardoiduista teknologioista huolimatta pilviteknologiaan ja pilvipalveluihin liittyy monia osa-alueita, joissa standardointi olisi välttämätöntä. Vaquero *et al.* (2009) mukaan useat näistä osa-alueista ovat palveluntarjoajien sisäisiä, liikesalaisuuksiin verrattavissa olevia ratkaisuja.

Chow *et al.* (2009) mukaan standardoinnin avulla voitaisiin välttää erilaiset yhteensopivuusongelmat sekä tiedon lukkiutuminen yhteen formaattiin jonkin yksittäisen palveluntarjoajan ongelmatilanteessa. Erityisesti pilviteknologian turvallisuutta pohdittaessa erilaiset standardit tulisi ottaa huomioon jo palvelujen kehityksen alkuvaiheissa — on kyseessä sitten pilviteknologian ylimmät sovelluskerrokset tai alimmat fyysisiä laitteita sisältävät kerrokset.

Boden *et al.* (2009) mukaan niin sovellus- kuin arkkitehtuurisuunnittelussa on tärkeää huomioida erilaiset standardit turvallisuuden takaamiseksi. Jensen *et al.* (2009) painottavat myös internet-selaimien turvallisuuden kehittämistä useiden pilvisovellusten ollessa loppukäyttäjälle selainpohjaisia. Kaufmanin (2009) mukaan on relevanttia pohtia myös globaalin ulkoistamisen vaikutuksia pilvipalveluihin. Tästä syystä tulisi huolellisesti selvittää eri maiden lakien vaikutukset tiedon liikkuessa yli valtiorajojen.

Standardoinin ohella tietoturvan ja laadun kehittämiseksi sekä riskien minimoimiseksi pilvipalveluissa, on yhtä tärkeää kehittää luotettavia salaustekniikoita tietosuojan varmistamiseksi. Seuraavissa luvuissa 4.1 – 4.3 käsitellään tietoaineiston suojaukseen liittyviä salaustekniikoita kuten symmetrinen ja epäsymmetrinen salaus sekä tietosuojaan liittyvää kehitystä ja tutkimusta. Luvussa 4.4 käsitellään lyhyesti pilvipalveluihin liitty-

viä standardeja ja niiden kehittämistä sekä luvussa 4.5 tietosuojaan liittyvää riskien- ja laadunhallintaa.

4.1 Tietoaineiston suojauksen salaustekniikoita

Tietoaineiston tietosuojan varmistamiseksi pilvipalvelualustoilla käytetään salaustekniikoita, jotka pohjautuvat joko tietokoneella tapahtuvaan bittien sekoittamiseen (symmetriset salaukset) tai matemaattiseen laskentaan (epäsymmetriset salaukset). Symmetrisessä tekniikassa esimerkiksi AES (Advanced Encryption Standard)-salaus käytetään samaa avainta sekä viestin salaukseen että salauksen purkuun, kun taas epäsymmetrisessä esimerkiksi RSA (Rivest, Sharmir, Adleman)-salaus käytetään eri avaimia: julkista avainta viestin salaukseen ja yksityistä avainta viestin purkamiseen (Järvinen 2003). Symmetrinen ja epäsymmetrinen salaus on kuvattu tarkemmin luvussa 4.2.

Salaus (engl. Cryptography) on yleisin tekniikka varmistaa turvallinen kommunikaatioyhteys kahden osapuolen välillä. Jos esimerkiksi A ja B lähettävät sanomia toisilleen ja he eivät halua toisten lukea tai muuttaa heidän viestien sisältöä, tämä tarkoittaa, että he haluavat turvallisen kommunikaatioyhteyden. Viestinnässä käytettään siirtovälinettä T, jos A lähettää viestin B:lle T:n kautta. Kolmas osapuoli, joka haluaa häiritä viestintää, muuttamalla viestiä kutsutaan tunkeutujaksi I. Kun viesti on matkalla kohti päämäärää, on se vaarassa joutua tunkeutujalle I, joka voi suorittaa Pfleeger *et al.* (2006) mukaan seuraavia toimenpiteitä:

- estää viestin perille menon, jolloin saatavuutta on rikottu
- lukea (salakuunnella) viestin sisällön, jolloin luottamuksellisuutta on rikottu
- muuttaa viestin sisältöä, jolloin viestin eheyttä on rikottu
- väärentää viestin tai esittää lähettäjää A ja lähettää viestin B:lle. Tämä rikkoo myös viestin eheyttä

Viestinnässä kahden osapuolen välillä viestin tietoturvaa voidaan rikkoa edellä mainitulla neljällä tavalla. Salaustekniikoilla voidaan välttää edellä mainittuja tietoturvaongelmia (Pfleeger *et al.* 2006).

Salauksessa käytettäviä tekniikoita ovat viestin salaaminen ja purkaminen. Salauksessa E viesti P muutetaan ihmisen ymmärtämättömään muotoon. Viesti voidaan muuttaa takaisin ihmisen ymmärtämään muotoon purkamalla D salaus. Järjestelmä, joka salaa ja purkaa viestin kutsutaan salausjärjestelmäksi.

Viesti $P = < Terve\ Maailma >$ salataan $C = E(P) = <\#, \%, g, i, u, y, m, n, \{, :, ? >$, jossa C on salattuviesti ja vastaavasti viesti puretaan $P = D(C) = < Terve\ Maailma >$.

Salausjärjestelmissä avainta K käytetään algoritmin kanssa, jotta viesti voidaan salata ja purkaa. Pfleeger *et al.* (2006) mukaan käytettäessä salauksessa samaa avainta sekä salauksessa että purkamisessa, silloin salausprosessia kutsutaan symmetriseksi salaukseksi ja avainta K kutsutaan symmetriseksi avaimeksi. Tässä tapauksessa salaus- ja purkamisalgoritmit ovat symmetrisiä ja niitä voidaan tarkastella käänteisinä toimintoina toisiinsa nähden. Yleinen merkitsemistapa on $C = E(K, P)$ ja $P = D(K, C)$ ja salausjärjestelmää merkitään $P = D\big(K, E(K, P)\big)$ [51].

Pfleeger *et al.* (2006) mukaan salausavaimen ollessa eri kuin purkamisavain, silloin salausprosessia kutsutaan epäsymmetriseksi. Epäsymmetrisessä salauksessa käytetään kahta avainta, jossa salausavainta kutsutaan yksityiseksi avaimeksi K_E ja purkamisavainta kutsutaan julkiseksi avaimeksi K_D. Yleinen merkitsemistapa on salaukselle $C = E(K_E, P)$ ja purkamiselle $P = D(K_D, C)$. Salausjärjestelmää merkitään vastaavasti $P = D(K_D, E(K_E, P))$ [51].

Tietoaineiston suojaamiseksi pilvessä on olemassa erilaisia salaustekniikoiden alalajeja kuten yksinkertainen salaus, toiminnallinen salaus, salaisen avaimen jakaminen, turvallinen monen osapuolen laskenta, täysin homoforminen salaus ja purkamattoman tietoaineiston käsittely (Furukawa *et al.* 2013).

- Yksinkertainen salaus (engl. Simple encryption): tietoaineisto salataan käyttäjän salaisella avaimella ennen tallentamista pilventallennustilaan. Kuitenkin use-

amman käyttäjän tapauksessa tulee salainen avain jakaa käyttöoikeuksien mukaisesti.

- Toiminnallinen salaus (engl. Functional encryption): Salausmenetelmä mahdollistaa useamman käyttäjän pääsynvalvonnan ja salauksen jaettuun tallennustilaan. Menetelmässä generoidaan salainen teksti, joka määrittelee käyttäjät, jotka voivat purkaa salauksen esimerkiksi käyttäjän tehtävän mukaan tai käyttäjä kuuluu tiettyyn käyttäjäryhmään. Salauksen purkaminen on mahdollista käyttäjille, jotka täyttävät tietyt määritellyt ehdot. Jos käyttäjän oikeuksia halutaan muuttaa, on välttämätöntä uudelleen generoida salainen teksti.
- Salaisen avaimen jakaminen (engl. Secret sharing): Tässä menetelmässä tietoaineisto hajautetaan useamman pilven tallennustilaan, siten että alkuperäisen tietoaineiston luottamuksellisuus voidaan turvata vaikka tietoaineisto vuotaa mihin tahansa pilvipalveluun. Menetelmässä tietoaineisto muunnetaan useampaan osaan, jossa alkuperäistä tietoaineistoa ei voida palauttaa, ellei ole kerätty tietty määrä tietoaineiston osia. Kukin pilven tallennustila kontrolloi käyttäjän pääsyä tietoaineistoon ja vaikka jokin pilvipalvelu kadottaisi osan tallennetusta tietoaineistosta, voidaan alkuperäinen tietoaineisto palauttaa muihin pilvipalveluihin tallennetuista tietoaineiston osista. Lisäksi ratkaisu mahdollistaa väärennöksen tunnistusmekanismin tietoaineiston eheyden varmistamiseksi.
- Turvallinen monen osapuolen laskenta (engl. Secure multi-party computation): Tämä teknologia mahdollistaa satunnaisen tietoaineiston käsittelyn. Sen jälkeen kun tietoaineisto on jaettu useampaan pilveen hyödyntämällä salaisen avaimen jakamista, pilvipalvelut voivat generoida alkuperäisen tietoaineiston yhteistyössä satunnaisella laskennalla palauttamatta jaettua salattua tietoaineistoa. Salausprosessi on tavallisesti hidas ja jos käyttäjät voivat hakea alkuperäisen tietoaineiston itse pilvestä, on paljon yksinkertaisempaa, jos he lukevat tietoaineiston ja sen jälkeen suorittavat salausprosessin itse.
- Täysin homomorfinen salaus (engl. Fully homomorphic encryption): Salaustekniikka mahdollistaa käsittelemään tietoaineistoa pilvessä avaamatta salausta. Toisin kuin tietoaineiston käsittely turvallisen monen osapuolen laskennassa, tietoaineisto käsittely on mahdollista vain yhdessä pilvessä. Salaustekniikan ongelmana on hidas käsittelynopeus ja salattua tietoaineistoa voi hyödyntää ainoastaan käyttäjä, joka omistaa salaisen avaimen.

- Purkamattoman tietoaineiston käsittely (engl. Processing Non-decrypted data): Salaustekniikka käsittelee tietoaineistoa yhdessä pilvessä hyödyntämällä täysin homomorfista salausta. Furukawa *et al.* (2013) mukaan salaustekniikan ongelmaksi muodostuu yhteisten palvelujen käyttö esimerkiksi sovellukset, jotka hyödyntävät tilastollista laskentaa, avainsanahakuja, relaatiotietokantoja. Tämä sen vuoksi, että salauksen purkaminen on rajattu vain yhdelle käyttäjälle.

Täysin homoformisen ja purkamattoman tietoaineiston käsittelyn salauksessa on ongelmana yksi salausavain, jolla vain yksi käyttäjä voi hyödyntää tietoaineistoa avaamatta purkausta. Furukawan *et al.* (2013) mukaan tämä ongelma voidaan kuitenkin kiertää hyödyntämällä salaustekniikkaa, jota kutsutaan välimuistin uudelleen salaukseksi (engl. proxy re-encryption). Salaustekniikka mahdollistaa useamman käyttäjän käsittelemään pilveen salattua tietoaineistoa.

Luvussa 5.3 kuvataan tarkemmin muun muassa homoformista salaustekniikkaa, jota pidetään lupaavana tekniikkana varmistaa tietoaineiston tietosuojaa koska salausta ei tarvitse purkaa missään käsittelyn vaiheessa.

4.2 Tietoaineiston suojauksen keskeiset algoritmit

Erilaiset salaustekniikat hyödyntävät tietoaineiston suojaamiseksi pilvipalveluissa pääsääntöisesti yleisemmin hyväksitunnettuja salausalgoritmeja kuten RSA (Rivest, Shamir, Adleman) tai AES (Advanced Encryption Standard) tietoaineiston eheyden ja luottamuksellisuuden varmistamiseksi. AES-salaus on kaupallisten markkinoiden yleisesti hyväksymä salausalgoritmi tuotettaessa esimerkiksi pilvipalveluja kuluttajille ja yrityksille. AES-salausratkaisu täyttää FIPS 197 tietoturvavaatimukset (NIST 2014). Katso sivu 38, taulukko 2.

Arkaluontoisia tietoaineistoja käsiteltäessä, jotka on luokiteltu esimerkiksi suojaustaso III, vaaditaan salausratkaisulta, että sen tietoturvallisuus on hyväksytty ja tarkastettu kyseessä olevalle tasolle (KATAKRI 2011). Kansallisella tasolla salausratkaisuja hyväksyy kyberturvallisuuskeskuksen NCSA-toiminto (Viestintävirasto 2014).

4.2.1 RSA-salaus

RSA-salaus on maailmanlaajuisesti tunnetuin ja käytetyin salausjärjestelmä. RSA-salausalgoritmin ovat kehittäneet Ron Rivest, Adi Shamir ja Len Adleman Massachusetts teknillisessä korkeakoulussa (MIT) vuonna 1977 ja se julkaistiin vuonna 1978. RSA on epäsymmetrinen salaustekniikka, jossa julkisella avaimella luodaan salattuja viestejä, jotka voidaan purkaa yksityisellä avaimella. Julkinen avain voidaan julkaista kaikille mutta yksityinen avain pidetään salattuna. Myöskään yksityistä avainta ei voida johtaa julkisesta avaimesta.

RSA:n turvallisuus perustuu olettamukseen, jonka mukaan erittäin suurien alkulukujen (jaollinen vain itsellään) tulon tekijöihin jako on vaikeaa. Kyseessä on yksisuuntainen modulaarifunktio, joka on helppo laskea mutta todella hankalaa ja aikaa vievää laskea taaksepäin.

Peter Shor osoitti jo vuonna 1994, että kvanttitietokone voisi periaatteessa suorittaa tekijöihin jaon polynomisessa ajassa (Mermin 2006). Jos (tai kun) kvanttitietokoneista tulee käytännöllisiä, Shorin algoritmi tekee RSA:sta vanhentunutta teknologiaa.

4.2.2 AES-salaus

AES (Advanced Encryption Standard) on vuonna 2001 avoimen kansainvälisen kilpailun voittanut Rijndael-salausmenetelmä. AES hyväksyttiin myös Yhdysvaltojen viralliseksi salausstandardiksi vuonna 2001 (Järvinen 2003). Rijndaelin suunnittelussa otettiin huomioon kolme kriteeriä. Ensinnäkin sen tulisi kestää kaikkia tunnettuja hyökkäyksiä. Lisäksi sen tulisi sopia moniin eri käyttökohteisiin, sekä nopeutensa, että koodin tiiviyden puolesta.

Useimmissa salausalgoritmeissa kierrosmuunnos tehdään käyttämällä Feistelin rakennetta. Rijndaelissa ei käytetä kierrosmuunnoksessa Feistelin rakennetta, vaan muunnos koostuu kolmesta erillisestä muunnoksesta, joita kutsutaan kerroksiksi. Nämä kerrokset ovat nimeltään lineaarinen sekoituskerros, epälineaarinen kerros ja avaimenlisäyskerros (Rijmen *et al.* 1999).

AES on symmetrinen lohkosalausjärjestelmä, jossa avaimen pituus voi olla mikä tahansa 32:n monikerta ja lohkon koko on 128 bittiä. AES:ssa on käytössä vain yksi 256 alkion S-laatikko, mikä tekee siitä nopean. Salaus muodostuu kierrosavaimien luomisesta ja kierrosfunktiosta. Kierrosfunktio koostuu neljästä erillisestä tilaa muokkaavasta funktiosta: SubBytes, ShiftRows, MixColumns ja AddRoundKey. Kierrosfunktiota suoritetaan sellaisenaan Nr-1 kertaa, viimeisen kierroksen poiketessa hieman aikaisemmista. Viimeisellä kierroksella MixColumns-funktio jätetään kokonaan pois. Tarvittavien kierrosten määrä riippuu AES-standardissa salausavaimen pituudesta. Kierroksia voi olla 10, 12 tai 14, salausavaimen pituuden ollessa vastaavasti 128, 192 tai 256 bittiä pitkä (FIPS 2001).

4.3 Tietoaineiston suojauksen kehitys ja tutkimus

Pilven tallennustilan tietosuojan varmistamiseen liittyvä kehitys ja tutkimus on keskittynyt tutkimaan miten käyttäjä voi tallentaa pilveen tietoaineistoa niin, että sen luottamuksellisuus voidaan turvata tietojen paljastumatta muille tahoille esimerkiksi pilvipalvelun tuottajalle tai kun käytetään kolmannen osapuolen tekemää auditointia tietoturvan varmistamiseksi pilvessä. Seuraavassa kuvataan joitakin salaustekniikoiden alalajeja, jotka ovat nousseet viime vuosina uudelleen tutkimuksen keskiöön tietoaineiston tietosuojan varmistamiseksi.

4.3.1 Homomorfinen salaus

Luottamuksellisuuden suojauksessa salausalgoritmien tutkimuksen keskiössä on muun muassa homomorfinen salaus, joka on saanut paljon huomioita kirjallisuudessa ja julkaisuissa viime vuosina (Gentry 2010). Gentryn (2009) alkuperäinen salausjärjestelmä ja sen muunnokset osoittautuivat olevan tehokkuuden pullonkauloja (Coron *et al.* 2011; Gentry *et al.* 2011; Smart *et al.* 2010; Smart *et al.* 2012). Myöhemmät toteutukset laajensivat viimeisempien algoritmien etuja (Brakerski *et al.* 2011; Brakerski *et al.* 2011a), jotka johtivat parempiin täysin homoformisen salausjärjestelmän toteutuksiin, samoin kuin uudet algebralliset mekanismit paransivat kaiken kaikkiaan näiden salausjärjestelmien tehokkuutta (Gentry *et al.* 2012; Naehrig *et al.* 2011; Smart *et al.* 2012). Homoforminen salaus voidaan jakaa additiiviseen ja moninkertaistavaan homoformismiin. Salaus, joka tukee molempia sanotaan olevan täysin homoforminen salaus.

Homoformismi sana tulee muinaisen kreikan kielen sanasta ”homos”, jolla tarkoitetaan ”samaa” ja sana ”morphe”, jolla tarkoitetaan ”tilaa”. Abstraktissa algebrassa homoforminen ymmärretään rakenteen säilyttäväksi kartaksi kahden algebrallisen rakenteen välillä kuten ryhmät, renkaat ja vektoriavaruudet. Esimerkiksi $f(x) = 3x$ on homomorfismi, sillä $f(a + b) = 3(a + b) = 3a + 3b = f(a) + f(b)$.

Homomorfisen salauksen kehittivät Rivest, Adleman ja Dertouzous vuonna 1977 hiukan myöhemmin RSA-salauksen keksimisen. Homomorfisen salauksen perusajatuksena on käsitellä salattua tietoaineistoa ilman, että salausta tarvitsee purkaa. Esimerkiksi alkuperäinen teksti on m, josta salauksen E jälkeen saadaan salattu teksti e ja käänteisesti purkamisoperaation D jälkeen saadaan alkuperäinen teksti m. Nyt on kaksi toimintofunktiota f ja F. Sovelletaan f alkuperäiseen tekstiin ja F salattuun tekstiin, saadaan $F(e) = E(f(m))$, josta F avulla saadaan salatun tekstin tulos $f(m)$. Toisin sanoen on mahdollista rakentaa salausjärjestelmä, jossa käyttäjä voi käsitellä salatun tekstin tulosta $f(m)$ mutta ei voi saada mitään tietoa alkuperäisestä tekstistä m. Rivest *et al.* mukaan RSA on moninkertaistava homomorfinen salausjärjestelmä (Rivest *et al.* 1978).

Esimerkki RSA:n moninkertaistavasta homomorfisesta salauksesta, jossa A lähettää viestin B:lle:

A valitsee 2 suurta alkulukua $p = 3$ ja $q = 7$
A laskee $n = p \cdot q = 3 \cdot 7 = 21$
A laskee $\varphi(n) = (p - 1) \cdot (q - 1) = 2 \cdot 6 = 12$
A valitsee $a = 2\ joukosta\ \{2, \ldots, 7\}$
A laskee $b = a^{-1}\ mod\ \varphi(n) = 3^{-1}\ mod\ 12 = 8$
A valitsee $m_1 = 4\ ja\ m_2 = 6$
A salaa $c_1 = m_1^a\ mod\ n = 4^3\ mod\ 21 = 1\ mod\ 21$
A salaa $c_2 = m_2^a\ mod\ n = 6^3\ mod\ 21 = 6\ mod\ 21$
A lähettää viestin B:lle $c_1 = 1, c_2 = 6$
B laskee $c_3 = c_1 \cdot c_2 = 1 \cdot 6\ mod\ 21 = 6\ (mod\ 15)$ ja lähettää A:lle $c_3 = 6$
A purkaa B:n viestin $c_3^b\ mod\ n = 6^8\ mod\ 21 = 15\ mod\ 21$

Gentry (2009) esittää, että esimerkiksi annetulla julkisella avaimella $pk = (N, e)$ ja salauksella $\{\varphi_i \leftarrow \pi_i^e \ mod \ N\}$, voidaan tehokkaasti laskea $(\prod i \ \pi_i)^e \ mod \ N$ salakirjoitus, jossa salataan alkuperäinen teksti. Bajpai *et al.* (2014) mukaan RSA on kuitenkin homomorfinen ainoastaan kertomisen suhteen. Valitettavasti Rivest, Adleman ja Dertouzous alun perin kehittämä homomorfinen salaus murrettiin joitakin vuosia sen keksimisen jälkeen (Brickell *et al.* 1987).

Homoformisessa salauksessa voidaan tietoaineisto teoriassa salata asiakassovelluksessa ja sen jälkeen tallentaa pilven tallennustilaan. Ainoastaan käyttäjällä on purkausavain. Gentry (2009) huomauttaa, että vaikka salaus kasvattaa käsittelyaikaa, ovat hyödyt kuitenkin suuremmat luottamuksellisuuden ja tietoaineiston eheyden näkökulmasta.

Vaikka homoforminen salaus keksittiin jo vuonna 1977, ei sitä ole voitu Gentry *et al.* (2012) mukaan hyödyntää sen vaatiman laskentatehon vuoksi kuin vasta viime vuosina kun tietokoneiden laskentateho ja muistinopeudet ovat kasvaneet.

Gentry (2009) on esittänyt väitöskirjassaan täysin homomorfiseen salaukseen perustuvan järjestelmän, jossa tietoaineisto salataan pilventallennustilaan. Tietoaineiston salausta ei tarvitse purkaa sen käsittelyn aikana, ainoastaan käyttäjä joka omistaa salaisen avaimen voi käsitellä salattua tietoaineistoa. Käyttäjä voi myös lähettää salattuja kyselyjä palvelimelle sen tuntematta kyselen sisältöä, myös tietoliikenne asiakkaan ja palvelimen välillä on salattu, joten myös liikenteen salakuuntelu ei ole mahdollista. Wang *et al.* (2013) mukaan symmetrinen homomorfinen salaus mahdollistaa myös turvallisen tietoaineiston auditointipalvelujen hyödyntämisen muun muassa hyödyntämällä autentikoinnissa julkiseen avaimeen pohjautuvaa homoformista lineaarista autentikaatiota koska kolmannen osapuolen tekemässä auditoinnissa voidaan käsitellä suoraan salattua tietoaineistoa. Symmetrinen salaus vähentää myös palvelimen suorittimen kuormitusta.

4.3.2 Salaisen avaimen jakaminen

Salaisen avaimen jakaminen viittaa menetelmään hajauttaa avain tietyn valitun ryhmän kanssa, jokainen joka on allokoitu jakamaan salaista avainta. Salainen avain voidaan koostaan ainoastaan tietystä määrästä jakoja, jotka on yhdistetty yhteen. Salaisen avai-

men jakamisen kehittivät toisistaan riippumattomasti Adi Shamir ja George Blakley vuonna 1979.

Blakleyn (1979) mukaan salausjärjestelmä määrittelee salaisen avaimen jakamisen useampiin osiin pisteinä n-ulotteisessa avaruudessa ja jakaa jaot jotka vastaavat hypertasoa, joka leikkaa pistettä. Mikä tahansa n tällaisella hypertasolla määrittelee pisteen, kun taas vähemmän kuin n hypertasoja jää vähintään yhtä astetta vapaaksi ja jättää siten pisteen määrittelemättä.

Vastaavasti Shamirin salaisen avaimen järjestelmä esittää salaisen avaimen n-aseteisen polynomin y-leikkauspisteenä ja jaot vastaavat pisteitä polynomissa (Shamir 1979).

Shamirin (1979) mukaan salaisen avaimen jakaminen protokolla on esimerkki salausprotokollasta, jossa on tarve suojata yhteisesti jaettua tietoaineistoa verkossa. Esimerkiksi oletetaan, että väärinkäytösten ehkäisemiseksi yhdelläkään pankin työntekijällä ei ole mahdollista yksistään avata pankin turvaholvia. Sen sijaan kullekin työntekijälle on annettu pala salasanaa holvin avaamiseksi. Kun k työntekijää yhdistävät tiedon palat, voivat he yhdessä koota salasanan ja avata holvin. Kuitenkaan, $k - 1$ työntekijällä ei yksistään ole riittävästi tietoa koko salasanasta niin, että $k - 1$ työntekijää voisivat varastaa pankin rahat.

Koodataan pala tietoa l-bittisenä binäärilukuna $a_{l-1}2^{l-1} + \cdots + 2_{a1} + a_0$ missä $a_i \in \{0,1\}$. Jos jaettava viesti on liian pitkä, voi sen jakaa pienempiin osiin niin, että kukin vaatii vähemmän kuin l-bitiä kirjoitukseen. Viesti voidaan tulkita äärellisenä kunnan elementtinä F_{2^l}. Jos viesti kuuluu $x \in F_{2^l}$, voidaan laskea mikä tahansa polynomi $c_0 + c_1x + \cdots + c_nx^n \in F_{2^l}$ ja käyttää Lagrangen interpolointi teoriaa: jos F on kunta ja $(x_i, y_i), \ldots, (x_n, y_n)$ ovat pistepareja kunnassa F_2, silloin on olemassa yksikäsitteinen polynomi $p(x) = c_{n-1x^{n-1}} + \cdots + c_0$ astetta $n - 1$ kuten $p(x_i) = y_i$, jossa $i = 1, \ldots n$ (Shamir 1979).

Mitä tällä on tekemistä salaisen avaimen jakamisen kanssa? Oletetaan, että koodataan salainen avain s -bittisenä lukuna kunnassa F_{2^l} ja oletetaan edelleen, että s halutaan ja-

kaa n ihmisten joukossa 1, ... n. Halutaan, että he voivat uudelleen koota salaisen avaimen s, jos k ihmistä yhdessä tekevät yhteistyötä mutta eivät saa yhtään tietoa, jos vähemmän kuin k ihmistä jakavat tiedon. Nyt generoidaan $k-1$ satunnaislukua $c_1, \ldots, c_{k-1}$ yhtäläisesti kunnasta F_{2^l} ja tarkastellaan polynomia $f(x) = s + c_1 x + \cdots + c_{k-1} x^{k-1}$. Kukin henkilö i, saa jaon $f(i)$.

4.3.3 Turvallinen monen osapuolen laskenta

Turvallinen monen osapuolen laskenta on salaustekniikoiden alalaji, jonka Andrew Yao (1982) esitteli vuonna 1982. Tämän menetelmän päämäärä on luoda menetelmä, joka mahdollistaa useamman osapuolen yhdistämään laskentatoiminnot syötteisiinsä ja samalla pitämään nämä syötteet yksityisinä. Tämä menetelmä on tärkeä alalaji salaustekniikoissa ja jota on läheisesti viitattu nollatiedon ideaan.

Yleisesti turvallinen monen osapuolen laskenta viittaa tietokonejärjestelmään, jossa useat osapuolet haluavat yhteisesti käsitellä salaista tietoa mutta eivät halua paljastaa tietoa toiselle osapuolelle. Esimerkiksi kaksi osapuolta jotka omistavat jotakin salaista tietoa x ja y haluavat yhteisesti käsitellä jonkin toiminnon $f(x, y)$ paljastamatta mitään tietoa x:stä ja y:stä toiselle muuta kuin sen mitä voidaan järkevästi päätellä tuntemalla tosiasiallinen $f(x, y)$ arvo. Wenliang *et al.* mukaan ”Järkevästi päätelty” on usein tulkittu yhtäläisenä tietojenkäsittelynä polynomisen ajan kanssa (Wenliang *et al.* 2002).

4.4 Pilvipalvelujen standardien kehittäminen

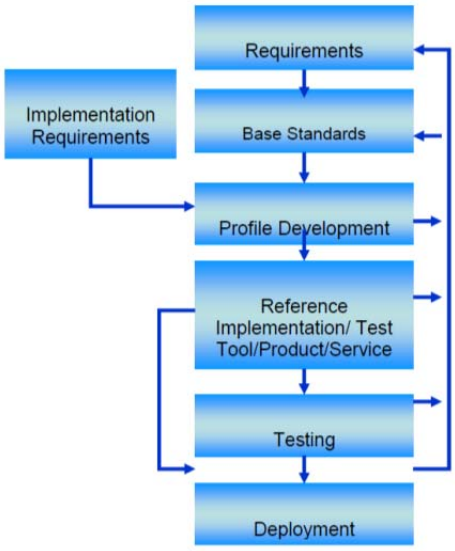
Alku vuonna 2011 yhdysvaltain valtion teknologia ja standardointi instituutti (The National Institute of Standards and Technology, NIST) käynnisti työryhmiä luodakseen teknisesti suuntautuneen strategian ja standardeihin perustuvan ohjeistuksen pilvipalveluiden teknologian ja tietoturvan toimeenpanohankkeelle. NIST käynnisti seuraavat työryhmät käsittelemään ja pohtimaan asiaa:

- Pilvilaskennan viitearkkitehtuuri ja luokitus
- Pilvilaskennan standardien käyttöönoton nopeuttaminen
- Pilvilaskennan tietoturva

- Pilvilaskennan standardoinnin tiekartta
- Pilvilaskennan liiketoiminnan kohde käyttötapaukset

NIST kiinnitti standardointityössä erityisesti huomion yhteensopivuuteen, siirrettävyyteen ja tietoturvaan (NIST 2014).

NISTin pilvilaskennan viitearkkitehtuuri on yleinen ylemmän tason konseptuaalinen malli, joka on voimakas työkalu keskusteltassa pilvilaskennan vaatimuksista, rakenteista ja toiminnoista. Pilvilaskennan standardien elinkaari kuvaa tiedon ja tietoliikenne standardien elinkaaren (kuva 10), joka on korkeamman tason käsite tavoista, jolla IT-standardit on kehitetty ja menetelmät joilla standardipohjaiset IT-tuotteet, prosessit ja palvelut on kehitetty (NIST 2014).



Kuva 10. *IT standardien elinkaari (NIST 2014).*

Myös muutkin tahot kuin NIST ovat kehittämässä pilvilaskennan standardointia kuten Cloud Computing Standards Development Organizations (SDO), joka antaa tukea pilvilaskennan dokumentoinnin standardointiin, käsitteelliseen malliin, viitearkkitehtuuriin, yhteensopivuuden arviointiohjelmiin ja standardoinnin tiekarttoihin auttamalla pilvilaskennan ja sen sovelluksien kehittämisessä tietoliikenteessä, tiedonsiirrossa ja tietoturvassa.

4.4.1 Pilvipalvelujen tietosuojaan liittyvät standardit

Taulukoissa 1 – 3 on esitetty tärkeimpiä tietoturvaan liittyviä myös markkinoiden hyväksymiä standardeja pilvipalveluiden tuottamisessa. Taulukossa 1 on esitetty todentamiseen ja käyttöoikeuksien rajaamiseen liittyvät standardit ja taulukossa 2 luottamuksellisuuteen sekä taulukossa 3 eheyteen. Jotkin standardit ovat soveltavissa useampaan kategoriaan ja ovat tästä syystä listattu useammassa taulukossa.

Taulukko 1. *Todentaminen ja käyttöoikeuksien rajaamiseen liittyvät standardit (NIST 2014).*

Categorization	Available Standards	SDO	Status
Authentication & Authorization	RFC 5246 Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)	IETF	Approved Standard Market Acceptance
	RFC 3820: X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile	IETF	Approved Standard Market Acceptance
	RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	IETF	Approved Standard Market Acceptance
	RFC 5849 OAuth (Open Authorization Protocol)	IETF	Approved Standard Market Acceptance
	ISO/IEC 9594-8:2008 | X.509 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks	ISO/IEC & ITU-T	Approved Standard Market Acceptance
	ISO/IEC 29115 | X.1254 Information technology -- Security techniques -- Entity authentication assurance framework	ISO/IEC & ITU-T	Approved Standard
	FIPS 181 Automated Password Generator	NIST	Approved Standard Market Acceptance
	FIPS 190 Guideline for the Use of Advanced Authentication Technology Alternatives	NIST	Approved Standard Market Acceptance
	FIPS 196 Entity Authentication Using Public Key Cryptography	NIST	Approved Standard Market Acceptance
	OpenID Authentication	OpenID	Approved Standard Market Acceptance
	eXtensible Access Control Markup Language (XACML)	OASIS	Approved Standard Market Acceptance
	Security Assertion Markup Language (SAML)	OASIS	Approved Standard Market Acceptance

Taulukko 2. *Luottamuksellisuuteen liittyvät tietoturva standardit (NIST 2014).*

Categorization	Available Standards	SDO	Status
Confidentiality	RFC 5246 Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)	IETF	Approved Standard Market Acceptance
	Key Management Interoperability Protocol (KMIP)	OASIS	Approved Standard Market Acceptance
	XML Encryption Syntax and Processing	W3C	Approved Standard Market Acceptance
	FIPS 140-2 Security Requirements for Cryptographic Modules	NIST	Approved Standard Testing Market Acceptance
	FIPS 185 Escrowed Encryption Standard (EES)	NIST	Approved Standard Market Acceptance
	FIPS 197 Advanced Encryption Standard (AES)	NIST	Approved Standard Testing Market Acceptance
	FIPS 188 Standard Security Label for Information Transfer	NIST	Approved Standard Market Acceptance

Taulukko 3. *Eheyteen liittyvät tietoturva standardit (NIST 2014).*

Categorization	Available Standards	SDO	Status
Integrity	XML signature (XMLDSig)	W3C	Approved Standard Market Acceptance
	FIPS 180-4 Secure Hash Standard (SHS)	NIST	Approved Standard Market Acceptance
	FIPS 186-4 Digital Signature Standard (DSS)	NIST	Approved Standard Market Acceptance
	FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC)	NIST	Approved Standard Market Acceptance

4.4.2 Pilvipalveluiden tuottamiseen liittyvät muut standardit

Pilviteknologian tietoturvaan läheisesti liittyviä muita tietojenkäsittelystandardeja ovat esimerkiksi ISO/IEC 2510:2011, ISO/IEC 27001:2005, ISO/IEC 27002, ISO/IEC 13236 ja PCI DSS (Payment Card Industry Data Security Standard) –standardit (ISO 2015, PCI 2015) sekä Common Criteria- ja ITIL-kehysmallit, jotka ottavat huomioon luotettavuuteen ja käytettävyyteen liittyviä tekijöitä kehitettäessä tietojenkäsittelypalveluita ja –sovelluksia (ITIL 2015, Common Criteria 2015).

ISO/IEC julkaisee vielä vuonna 2015 kaksi uutta standardia ISO/IEC 27017 ja ISO/IEC 27018, jotka pohjautuvat ISO/IEC 27001 ja ISO/IEC 27002 standardeihin. Uudet standardit on kehitetty erityisesti pilvipalveluiden tietoturvan parantamiseksi. Standardien kehitys on suora vastaus Euroopan komission tavoitteelle tehostaa pilvipalveluiden käyttöönottoa Euroopassa talouden eri sektoreilla. Euroopan pilvipalveluiden strategia ja sen päämäärät julkaistiin vuonna 2012 ja ISO/IEC standardit ovat suora vastaus tähän pyrkimykseen (ISO 2015).

ISO/IEC 27001 antaa kehyksen tietoturvakontrolleille, joita voidaan soveltaa eri kokoisille organisaatioille luomaan tietoturvastandardien kehyksen. ISO/IEC 27002 mahdollistaa tarkoituksenmukaisen ISOI/IEC 27001 standardin kehyksen toteutuksen organisaatiossa. ISO/IEC 2017 standardi määrittelee ohjeet pilvipalveluiden tietoturvalliselle käytölle ja ISO/IEC 27108 standardi käsittelee yksityisyyden suojaan liittyviä asioita ja määrittelee käytännöt suojata luottamuksellista tietoaineistoa pilvipalveluissa (ISO 2015).

ISO/IEC 27002 standardissa käsitellään seuraavia tietoturvaan liittyviä osa-alueita, jotka täydentävät ISO/IEC 27017 ja ISO/IEC 27018 standardeja:

- Informaation tietoturvapolitiikoita
- Organisaation informaation tietoturvaa
- Henkilöstön tietoturvaa
- Omaisuuden hallintaa
- Pääsyn valvontaa
- Salausta
- Fyysistä tietoturvaa
- Käytön tietoturvaa
- Tietoliikenteen tietoturvaa
- Järjestelmien hankintaa, kehitystä ja ylläpitoa
- Toimittaja suhteita
- Informaation tietoturvatapahtumien hallinta
- Informaation tietoturva liiketoiminnan jatkuvuuden hallinnan näkökulmasta

- Määräystenmukaisuus (ISO 2015).

4.4.3 Pilvipalvelujen standardeihin liittyvät ongelmat

Pilvipalvelut ovat hajautetun tietotekniika-evoluution tulosta, jonka on mahdollistanut nopeat ja kustannuksiltaan edulliset tietoliikenne palvelut, käytännölliset ja suorituskseltaan korkeat virtuaalisointiteknologiat sekä kehittyneet ja vuorovaikutteiset web-teknologiat. Kuitenkin pilvilaskenta kohtaa suuria haasteita pilvipalveluita tuottavien toimittajien osalta. Nykyinen pilvipalveluiden standardointi ei huomioi standardoinnissa olevia aukkoja, jotka johtuvat uusista palvelumalleista, hajautettujen resurssien kontrolloinnista sekä omistajuuteen liittyvistä ongelmista (NIST 2014).

Hajautettujen resurssien ongelmana on, että palveluita käyttävällä kuluttajalla ei ole suoraa näkyvyyttä tietokoneresursseihin. Sen sijaan kuluttajan kommunikoivat pilvipalvelun tuottajan mahdollistamien palvelurajapintojen kautta kuten SaaS, PaaS ja IaaS saadakseen näkymän pilvipalvelun resursseihin. Rajapinnat voidaan luokitella kahteen tyyppiin 1) toiminnalliseen rajapintaan, joka laajentaa palvelun toimintoa ja 2) hallintarajapintaan, joka mahdollistaa kuluttajan hallitsemaan vuokrattua tietokoneresurssia (NIST 2014).

SaaS-palvelumallissa standardointi ei huomioi sovelluskohtaista tietoaineistoa ja metadataa yhdenmukaisuuden ja siirrettävyyden osalta (NIST 2014). Tämä on ongelma esimerkiksi sähköposti ja toimisto-ohjelmien tietoaineiston (formaatti) migratoinnin osalta pilvipalvelualustalle, jos se ei tue standardointia.

4.5 Tietosuojaan liittyvien riskien vähentäminen

Luvun 4 lopuksi käsitellään lyhyesti tietoturvariskien vähentämisen näkökulmasta keskeisempiä ja tärkeimpiä tiedon suojaamisen näkökulmia, joita ovat:

- luottamuksellisuus
- käytettävyys
- eheys

Hakala *et al.* (2006) määrittelevät tietoturvan tiedon arvoon perustuvan määritelmän ja laajennetun määritelmän avulla. Klassinen tapa määritellä tietoturvaa on käsitellä tiedon arvoa. Tähän liittyen luottamuksellisuudella tarkoitetaan tilannetta, jossa ”tietojärjestelmän tiedot ovat vain niihin oikeutettujen henkilöiden käytettävissä”. Käytettävyys on sen sijaan määritelty niin, että ”tiedot ovat saatavissa tietojärjestelmästä oikeassa muodossa riittävän nopeasti”. Eheydellä tarkoitetaan tietojärjestelmän tietojen paikkansapitävyyttä ja että tiedot eivät sisällä tahallisia tai tahattomia virheitä.

Hakalan *et al.* (2006) mukaan luottamuksellisuutta vaalitaan käyttäjätunnuksin ja salasanoin sekä erilaisten salausmenetelmien avulla. Käytettävyyttä ja eheyttä pyritään turvaamaan niin laitteistotason kuin ohjelmistoteknisin ratkaisuin. Aiemmin mainittu laajennettu määritelmä pitää sisällään edellisen kolmen lisäksi myös kiistämättömyyden ja pääsynvalvonnan. Kiistämättömyydellä tarkoitetaan varmuutta siitä, että tietojärjestelmää todella käyttää sama taho, joka on oikeutettu siihen ja että tallennettava tieto on luotettavaa. Pääsynvalvonnalla taas kontrolloidaan ja rajoitetaan organisaation tietojärjestelmän käyttöä. Ulkopuolisten tahojen pääsy tietojärjestelmään voidaan estää erilaisin laitteistollisin ratkaisuin (Hakala *et al.* 2006).

Chowin *et al.* (2009) mukaan pilviteknologiaan liittyvät riskit voidaan jakaa kolmeen kategoriaan: yleiseen turvallisuuteen, saatavuuteen ja kolmannen osapuolen olemassaoloon. Kategoriat ovat sovellettavissa aikaisemmin määriteltyyn tietoturvan klassiseen määritelmään. Tässä yhteydessä yleisen turvallisuuden kategoriaan voidaan ajatella kuuluvan ne ratkaisut, joilla tiedon eheys ja oikeellisuus turvataan. Saatavuuden ajatellaan olevan niitä käytettävyyden osa-alueita, joilla varmistetaan, että haluttu tieto on saatavilla. Kolmannen osapuolen olemassaolo on verrattavissa luottamuksellisuuden osa alueeseen. Pilvipalvelujen SaaS-palvelumallissa edellä mainittuja keskeisiä tietoturvariskejä voidaan minimoida rakentamalla palvelu siten, että se noudattaa luvussa 4.4.1 lueteltuja standardeja.

Subshini *et al.* (2011) esittää seuraavia näkökulmia tiedon luottamuksellisuuden, eheyden ja käytettävyyden parantamiseksi. Tiedon eheyttä hajautetuissa ympäristöissä, joissa on useita tietokantoja ja sovelluksia voidaan parantaa käyttämällä keskitettyä globaalia tapahtumienhallintaa. Kukin sovellus hajautetussa ympäristössä tulee kyetä jaka-

maan globaalit tapahtumat resurssienhallinnan kautta. Tähän liittyy kuitenkin ongelma koska SaaS-palveluiden sovellusten rajapinnat ovat XML-pohjaisia ja liikennöinti kuluttajalle hoidetaan http-protokolla hyödyntämällä web services -tyyppistä integraatiota kuluttajan ja pilvipalvelun tuottajan välillä. Http-protokolla ei kuitenkaan tue tapahtumapohjaista liikennöintiä tai takaa toimitusta. Tästä syystä web services -tyyppiset integraatiot hoidetaan sovellusrajapinnalla kuluttajalle. Subashini *et al.* (2011) mukaan web services -tyyppisiä integraatioita voidaan rakentaa tietoturvallisemmaksi hyödyntämällä WS-transactions ja WS-relibility standardeja (OASIS 2015) tapahtumien välittämiseksi tietoverkossa mutta monet pilvipalveluiden toimittajat eivät ole ottaneet näitä teknologioita käyttöön.

Chow et al. (2009) mukaan pilvipalvelun tuottamisen luottamuksellisuuteen liittyvä tekijät ovat ongelmallisia monistakin syistä; tiedon hajautuminen eri pilvipalveluiden tuottajien palvelimille, teollisuusvakoilu, tiedon lukkiutuminen tietyn palveluntuottajan formaattiin, pilvipalveluiden tuottajan mahdollinen erilainen lainsäädäntö sekä mahdolliset alihankkijoiden kautta toteutettavat palvelut ovat merkittäviä tekijöitä lisäämään epäluottamusta pilviteknologioita kohtaan.

Pilvipalveluiden kehittämisessä tekninen toimivuus on ensisijaisen tärkeää. Palveluiden teknisen toimivuuden varmistamiseksi riskitekijät huomioonottava suunnittelu voidaan jakaa ennakoiviin ja reaktiivisiin toimintamalleihin. Jensenin *et al.* (2009) mukaan pilvipalveluiden teknistä toimivuutta tarkasteltaessa on tärkeintä ottaa huomioon verkkopalveluihin liittyvä turvallisuus. Tähän liittyvät erityisesti tiedon luottamuksellisuus, eheys ja käytettävyys.

Tiedon suojaaminen ja salassapito on mahdollista toteuttaa monella eri tavalla pilviteknologiassa. Itani *et al.* (2009) esittävät tiedon suojaamisen myymistä palveluna, joka koostuu erilaisista metodeista hyödyntämällä kryptografiaa ja luotettavia kolmansia osapuolia. Chow *et al.* (2009) sen sijaan esittävät pilvessä olevan tiedon suojaamiseksi älykkään tietoaineiston menetelmän, jossa haluttu tietosisältö aukeaa käyttäjälleen ainoastaan, jos tietoaineisto havaitsee ympäristön turvalliseksi. Wang *et al.* (2009) mukaan turvalliseen pilviteknologiaan liittyy olennaisesti vahva salaus skaalautuvalla avainhal-

linnolla, käyttöoikeuksienhallinta, tiedon elinkaaren hallinta sekä järjestelmien saatavuus ja suorituskyky.

Pilvipalveluita tarjottaessa kuluttajille ovat käyttöoikeuksienhallinta ja pääsynvalvonta tärkeitä osa-alueita turvallisuuden takaamisessa. Todennus ja valtuutus toteutetaan pilvessä usein Public Key -infrastruktuurin ja X.509 SSL -sertifikaatin avulla (Youseff *et al.* 2008). Pilviteknologian perustuessa ulkoisiin tietojenkäsittelyresursseihin käyttäjät kirjautuvat ohjelmistotasolla pilveen, jolloin käytettävänä rajapintana on usein tavallinen internet-selain (Jensen *et al.* 2009). Siten internet-selaimien kehittäminen tietoturvalliseksi on ensisijaisen tärkeää käytettäessä pilvipalveluita. Internet-teknologiaa hyödyntävien pilvipalveluiden suojaamisessa XML-pohjaiset ratkaisut ovat usein melko tavallisia. Pervez *et al.* (2010) mukaan erilaiset Single Sign on -kirjautumiset ovat tyypillisiä ratkaisuja pilviteknologialle.

Sripanidkulchai *et al.* (2010) mukaan laajojen hajautettujen järjestelmien hyödyntämisen lisäksi pilviteknologiaan liittyvät oleellisesti myös saatavuuden ja ongelmanratkaisun näkökulmat. Saatavuuden turvaamiseksi pilviteknologiassa oleellisina osina ovat vaihtoehtoiset sisällöntoimitusverkostot, erilaiset kuormantasauskomponentit sekä automaattinen skaalaus. Edellistä saatavuutta turvaavat tekijät eivät välttämättä kuitenkaan riitä kokonaisen pilven kohdatessa ongelmatilanteen. Siten olisi erityisen tärkeää kehittää myös pilvien välistä saatavuutta parantavia ratkaisuja pilvipalveluita tarjoavien tahojen liiketoimintojen siitä kuitenkaan häiriintymättä (Sripanidkulchai *et al.* 2010). Saatavuuden vastakohtana voidaan pitää ongelmatilannetta, jossa pilvipalveluiden käyttö estyy kokonaan. Youseff *et al.* (2008) mukaan ongelmatilanteita varten pilvipalveluita tarjoavilla organisaatioilla tulisi olla toipumissuunnitelma palveluiden saattamiseksi nopeasti uudelleen toimintakuntoon.

Hakala *et al.* (2006, s.98) jakavat riskienhallintadokumentit toipumissuunnitelmaan ja valmiussuunnitelmaan. Toipumissuunnitelman avulla voidaan varautua toimimaan tietyllä tavalla määrittelyvaiheessa löytyneiden riskien realisoituessa, kun taas valmiussuunnitelma on laajempi dokumentti, poikkeustilanteita, kuten yhteiskuntaan tai ympäristöön liittyviä katastrofeja varten laadittu toimintasuunnitelma.

5 PILVIPALVELUIDEN TIETOSUOJAN VARMISTAMINEN

Pilvipalvelut tarjoavat valtavan määrän tallennustilaa ja resursseja pilvipalveluiden käyttäjille. Pilvipalvelun tuottajan tulee varmistaa käyttäjän tietoaineiston eheys ja virheettömyys pilvessä sekä tarjota jokin mekanismi, jolla se voi vakuuttaa käyttäjälle, että tietoaineisto on tallennettu pilveen turvallisesti ilman pelkoa tietoaineiston katoamisesta tai että sitä on muutettu.

Tietoaineiston säilytystila pilvessä on virtuaalinen hajautettu online-tilassa oleva tallennustila. Tietoaineiston tallennustilaa pilvessä voidaan käyttää web-palvelurajapinnan tai web-pohjaisen käyttöliittymän avulla. Eräs etu on sen joustavuus, skaalatutuvuus ja sitä voi käyttää samaan aikaan useat käyttäjät. Pilvipalveluiden käyttäjät saavat tarvittavan tallennustilan ja maksavat ainoastaan sen käytöstä. Pienet yritykset ja kuluttajat säästävät ylläpitokustannuksissa kun ei tarvitse investoida tallennuslaitteisiin ja ylläpitoon.

Maailman laajuisesti suurimpia pilvipalvelun tuottajia tallennustilan tarjoamisessa ovat Amazon, Google ja Microsoft. Amazon on tunnetuin tallennustilan tarjoaja pilvessä. Se tarjoaa tietoaineiston tallennustilaan kuluttajille ja yrityksille web-palvelurajapintojen kautta kuten REST, SOAP ja BitTorrent. Amazon S3 tallennustila on tarkoitettu suurille määrille tietoaineistoa aina 5 teratavuun saakka ja vähemmän tallennustilaa tarvitseville on tarjolla Amazonin SimbleDB tallennustila (Amazon 2014).

Pilvipalveluiden käyttäjät ovat kuitenkin riippuvaisia pilvipalveluiden tuottajien tarjoamista tallennuspalveluista saadakseen tallennettua tietoaineiston pilveen. Muthakshi *et al.* (2013) esittävät, että toisaalta pilveen ulkoistettu tietoaineisto on haavoittuvainen erilaisille sisäisille ja ulkoisille uhille tietoaineiston eheyden ja luottamuksellisuuden säilyttämiseksi.

Pilvipalveluiden hajaantuminen on myös kasvattanut pilvipalveluiden tuottajille erilaisia vaatimuksia suojata arkaluontoista tietoaineistoa kuten henkilökohtaisia tietoja. Pilvipalveluiden tietosuojan varmistamiseen liittyy vielä suuri joukko avoimia kysymyksiä, jotka ovat asettaneet pilvipalveluiden käyttäjille oikeutetun huolen tietoturvasta. Furukawa *et al.* (2013) mukaan käyttäjille on erittäin haasteellista kontrolloida tietoaineistoa suoraan pilvessä, joka aiheuttaa huolen tietoaineiston vuottamisesta ja väärinkäytöksistä.

Luvussa 5 käsitellään tietoaineiston salausta, kontrollointimekanismeja sekä kahta maailman laajuisesti johtavaa yhdysvaltalaisia tietoaineistojen suojaamiseen liittyvää tietoturvaratkaisua, joilla voidaan parantaa käyttäjän pilveen tallentaman tietoaineiston luottamuksellisuutta.

5.1 Tietoaineiston suojaus ja kontrollointi pilvipalvelussa

Tässä luvussa kuvataan yleisellä tasolla tietoaineiston suojaamista ja kontrollointia. Fyysisten laitteiden, järjestelmien, sovellusten, verkkoresurssien, ohjelmistorajapintojen, palomuurien ja niin edelleen teknisen tietoturvan lisäksi, tulee pilvipalveluiden tuottajien noudattaa erilaisia teollisuus-standardeja (katso luku 4.4), menettelyohjeita ja lakeja (katso luku 3.3) suojaamaan arkaluontoisia tietoja siirrettäessä tietoaineistoa pilveen (data in transmission) ja tallennettaessa tietoaineistoa (data at rest) pilven tallennuslaitteille.

Tarkasteltaessa tietoaineiston suojaamisen varmistamista virtuaalipalvelimilla, tulee tietoliikenteen ja tietoaineiston suojaamisen lisäksi asiakkaiden tietoaineisto pilvessä erottaa luotettavasti toisistaan pilven tallennustilassa luottamuksellisuuden varmistamiseksi. Tämän lisäksi tietoaineisto tulee myös voida turvallisesti siirtää ja tallentaa pilven tallennustilaan tietoaineiston eheyden säilyttämiseksi. Pilvipalveluiden tuottajien tulee myös varmistaa ja ehkäistä tietoaineistovuodot tai tietomurrot pilvessä.

Muthakshi *et al.* (2013) mukaan resurssien eristäminen pilvessä varmistaa osaltaan tietoaineiston turvallisen käsittelyn erottamalla prosessoreiden välimuistit virtuaalilaitteilla ja erottamalla nämä välimuistit edelleen virtuaalipalvelimen välimuistista.

Tietoaineiston suojaamiseksi pilven tallennustilassa tarvitaan tämän lisäksi suojaamista myös sekä sovellus- että verkkotasolla. Esimerkiksi CareStream Health (2011) mukaan tietoliikenneyhteys terveydenhuollon ja pilvipalveluntuottajan välillä perustuu SSL (Secure Socket Layer) pohjaiseen salaukseen sovellustasolla varmistamaan päästä päähän tietosuojan. Se myös estää tietoaineiston lukemisen kun se siirretään yli julkisen tietoverkon käyttäjän sovellukseen. CareStream käyttää tietoaineiston siirrossa Advanced Encryption Standard (AES) salausalgortimia (CareStream Health 2011).

Pilvipalveluiden tietoturvaa voidaan myös kontrolloida hyödyntämällä kolmannen osapuolen tekemiä tietoturva-auditointeja varmistamaan liiketoimintaprosessien ja valittujen tietoturvaratkaisujen vaatimuksenmukaisuutta. Tämän lisäksi pilvipalvelun tuottaja voi myös itse tehdä säännöllisesti pilven infrastruktuuriin verkon ja sovellusten läpitunkeutumistestejä hyödyntämällä parhaita käytäntöjä ja ohjeita (CSA 2014).

5.1.1 Tietoaineiston kontrollointi pilvessä

Harrington *et al.* (2003) mukaan pilvipalveluiden pääsynvalvonta ja tietoaineiston kontrollointi mekanismeja on kahdenlaisia: palvelinkeskeisiä, jossa käyttäjän tulee luottaa palvelimeen ja käyttäjäkeskeisiä, jossa tietoaineisto salataan asiakaskoneella taaten näin luottamuksellisuuden mutta tietoaineiston eheyttä ei voida kuitenkaan taata. Monissa palvelinkeskeisissä tietoaineiston kontrollointiratkaisuissa käyttäjän tulee konfiguroida pääsyvalvontamekanismi palvelimella, joka vaati jokaiselta käyttäjältä käyttäjätunnuksen. Käyttämällä salattua pääsynvalvontamekanismia, palvelin ei suoraan osallistu pääsynvalvontaan ja siten käyttäjät eivät tarvitse käyttäjätunnuksia. Tämä tekee tallennustilan käytöstä pilvessä joustavampaa.

Käyttäjäkeskeisessä salatussa pääsyvalvontamekanismissa tietoaineisto salataan paikallisesti asiakaskoneessa ennen sen tallentamista pilven tallennustilaan. Salauksen purkamista varten käyttäjän tulee siirtää tietoaineisto pilvestä paikallisesti asiakaskoneelle, jossa sen salaus puretaan. Tässä pääsynvalvontamekanismissa käytetään kahdenlaista salausmekanismia. Ensiksi salauksessa ja purkamisessa käytetään symmetristä salausta. Asiakassovellus salaa tietoaineiston paikallisesti käyttämällä symmetristä salausta ja sen jälkeen tallentaa salatun tietoaineiston pilveen. Jos asiakassovellus tai joku toinen val-

tuutettu asiakassovellus haluaa lukea tietoaineistoa, täytyy käyttää vastaavaa salausavainta tietoaineiston purkamiseksi. Toiseksi tietoaineiston salauksen ja purkamisen lisäksi, kaksi muuta tärkeää toimintoa suoritetaan tietoaineistolle nimittäin allekirjoitus ja varmentaminen. Näissä toiminnoissa käytetään epäsymmetristä salausmekanismia, jossa tarvitaan julkinen ja salainen avain. Tietoaineiston salauksen jälkeen generoidaan allekirjoitus, joka liitetään tietoaineistoon. Julkinen avain on luovutettu palvelimelle, jota käytetään tulevaisuudessa varmistamiseen kun tietoaineistoa muokataan (Harrington *et al.* 2003).

Harringtonin *et al.* (2003) mukaan käytettäessä salattua pääsynvalvontaa, jossa tietoaineisto on ensin salattu paikallisesti ja vasta sen jälkeen tallennettu pilveen, voidaan varmistaa tietoaineiston luottamuksellisuus ja eheys. Kuka tahansa voi saada salatun tietoaineiston mutta ainoastaan valtuutettu käyttäjä tai käyttäjät, joilla on tarvittavat salausavaimet voivat lukea tietoaineiston sisällön. Tämä takaa tietoaineiston luottamuksellisuuden. Kun valtuutettu käyttäjä (tai asiakassovellus) noutaa pilvestä allekirjoitetun tietoaineiston, varmistetaan ensiksi tietoaineiston eheys. Jos allekirjoituksen varmentaminen epäonnistuu, tiedetään tästä, että tietoaineistoa on ”peukaloitu”. Jos taas allekirjoituksen varmentaminen onnistuu, tiedetään vastaavasti, että tietoaineisto on eheä ja koskematon.

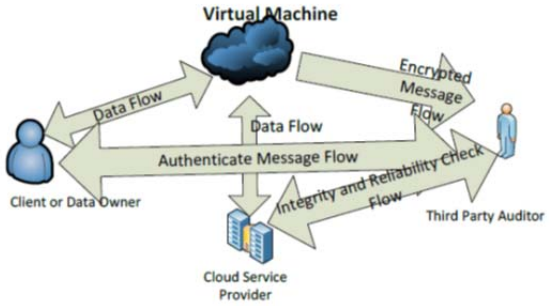
Tietoaineiston kontrolloimiseksi, käyttäjällä (tai asiakassovelluksella) on erilaisia oikeuksia pilveen tallennettuun tietoaineistoon. Jos käyttäjällä on julkinen ja symmetrinen avain, on hänellä lukuoikeudet tallennettuun tietoaineistoon, koska hän voi varmentaa tietoaineiston allekirjoituksen ja purkaa sen. Jos taas käyttäjällä on sekä julkinen, salainen ja symmetrinen avain, on hänellä sekä luku- että kirjoitusoikeudet tietoaineistoon ja hän voi purkaa salauksen muokkausta varten ja sen jälkeen uudelleen salata ja allekirjoittaa tietoaineiston.

Käyttäjäkeskeinen salattu pääsynvalvonta (datan kontrollointi) on tietoturvallisempi kuin palvelinkeskeinen, koska avainten hallinnointi on käyttäjällä. Kuitenkin tämän edellytyksenä on, että käyttäjä huolehtii riittävästä tietoturvasta kun avaimet tallennetaan paikallisesti asiakaskoneelle (Harrington *et al.* 2003).

5.1.2 Kolmannen osapuolen tekemä auditointi

Pilvipalveluiden käyttäjät voivat myös varmistua pilven tallennustilan tietoturvasta hyödyntämällä kolmannen osapuolen tekemää tietoturva-auditointia (engl. The third party auditor, TPA). TPA arvioi käyttäjän puolesta siirtotien ja tallennustilan tietoturvan luottamuksellisuuden ja eheyden näkökulmasta.

Pilvipalveluiden käyttäjät usein luottavat pilvipalveluiden tuottajien tarjoamaan tallennustilaan ja ylläpitoon pilvessä. Kuitenkin pilveen tallennettuun tietoaineistoon kohdistuu erilaisia tietoturvariskejä kuten tietojen korruptoitumista, tietojen varastamista, tietojen katoamista tai epäilys mahdollisuudesta, että pilvipalveluiden ylläpitäjät väärinkäyttävät pilveen tallennettua tietoaineistoa. Pilvipalveluiden käyttäjät voivat turvautua tällöin TPA:n tarjoamiin palveluihin varmistamaan pilveen ulkoistetun tietoaineiston tietoturvasta. Luvussa 5.2 käsitellään tietoturvaratkaisuja, jotka on rakennettu pilvi-infrastruktuurin päälle suojaamaan kuluttajan ja yritysten arkaluontoista tietoaineistoa.



Kuva 11. *Kolmannen osapuolen tekemä auditointi (Wang et al.2010).*

Kuvassa 11 pilvipalvelun käyttäjä tai käyttäjät (Client or Data owner) valtuuttaa kolmannen osapuolen auditoijan (Third Party Auditor, TPA) varmistamaan tai arvioimaan pilvipalvelun tuottajan (Cloud Service Provider, CSP) tarjoamien palveluiden kuten tallennuspalveluiden luotettavuuden tietoaineiston eheyden ja luottamuksellisuuden näkökulmasta. Tämän lisäksi TPA:n tulee olla luotettava taho, joka ei pääse käyttäjän tietoaineiston sisältöön tai kuormita käyttäjää palvelullaan.

Käyttäjä valtuuttaa TPA:n auditointioikeudet allekirjoittamalla sertifikaatin, jolla myönnetään TPA:n julkiselle avaimelle oikeudet. TPA tekee kaikki auditoinnit pilven

tallennustilaan tätä sertifikaattia vasten. Wang *et al.* mukaan yksityisyyden takaamiseksi käyttäjän tietoaineistoon, tulee TPA:n auditointiprotokolla taata seuraavat tietoturvavaatimukset (Wang *et al.*2010):

- julkinen auditoitavuus: TPA:lla on mahdollisuus varmistua tietoaineiston virheettömyydestä ilman koko tietoaineiston kopioa tai että tulee esittää lisäpyyntöjä käyttäjälle
- tallennustilan virheettömyys: varmistua, että pilvipalvelu on todella se taho, joka väittää olevansa
- yksityisyydensuoja: varmistua, että TPA ei voi saada auditointiprosessin aikana käyttäjän tietoaineistoa käyttöön tai nähtäväksi

Hyödyntämällä autentikoinnissa julkiseen avaimeen pohjautuvaa homoformista lineaarista autentikaatiota, voi TPA suorittaa auditoinnin pyytämättä käyttäjää siirtämää tietoaineistoa TPA:lle. Tämän lisäksi käyttämällä edellä mainitun salauksen yhteydessä satunnaista suojausprotokollaa (engl. Random Masking Protocol), ei TPA voi lukea käyttäjän tietoaineistoa (Wang *et al.*2010).

5.1.3 Fyysisen tason tietoturvan kontrollointi

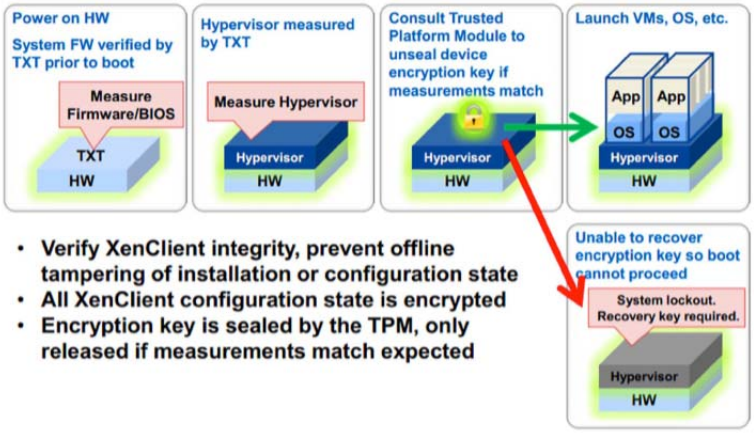
Tietoturvaa voidaan parantaa myös fyysisellä tasolla monella tavalla huomioimalla turvallisuuden valvonta datakeskuksessa esimerkiksi aidat, muurit, esteet, suojat, portit, elektroninen valvonta, fyysiset todentamismekanismit, vastaanotot, vartijat, hankkimalla valtuutus laitteistojen, ohjelmistojen tai tietoaineiston uudelleen sijoittamiseen tai siirtoon datakeskuksen ulkopuolelle, rajoittamalla datakeskuksessa henkilöstön ja ylläpitäjien fyysistä pääsyä tietoihin ja toimintoihin ja niin edelleen (CSA 2014).

Shpantzer (2013) esittää, että fyysistä tietoturvaa voidaan parantaa myös laitteistotasolla pilven infrastruktuurissa sekä virtuaali- ja mobiililaitteissa Trusted Platform Module-teknologialla (TPM), jonka toteutuksen IBM kehitti ja julkaisi vuonna 2003. Teknologian väitettiin olevan vastaus organisaatioiden arkaluontoisen tietoaineiston suojaamiseen. TPM-teknologialla voidaan tarkistaa tietokoneen käynnistymisen yhteydessä käynnistyslohko ja täyttääkö kone tietoturvavaatimukset ennen sen suorittamista.

TPM-teknologiaa kehitetään edelleen Trusted Computing Groupissa, jossa toimivat IBM:n lisäksi useita tietokone- ja laitevalmistajia kuten muun muassa AMD, Cisco, Dell, HP, Cisco, Infineon, Intel, Microsoft ja Juniper Networks. TPM-teknologiaa tukee maailmassa jo noin miljardi myytyä laitetta suojaamaan käyttäjän tietoaineistoa.

TPM 2.0 määrittely julkaistiin vuonna 2013 ja se tukee paremmin muistin ja suorituksen aikaista suojaa, jossa samassa laitteessa voi olla useita turvattuja toimintotiloja eri käyttötarkoituksille. TPM 2.0 määrittelyn mukaisia piirteitä tukevat muun muassa Intelin x86 ja ATOM prosessorit sekä muun muassa Nokia Windows 8 älypuhelin. TPM 2.0 määrittely täyttää myös NIST tietoturvavaatimukset NIST SP 800–147, 800–155, ja 800–164 alustoille.

TPM-teknologia (kuva 12) tukee virtuaalilaitteiden tietoturvaa myös laitteistotasolla. Alun perin Yhdysvaltain puolustusministeriölle suunniteltu SecureView on virtuaalityöpöytä, joka käyttää TPM- ja Intelin Trusted eXecution teknologiaa (TXT) käynnistämään virtuaalilaiteet huolellisesti kontrolloidussa ympäristössä.



Kuva 12. *TPM-teknologian hyödyntäminen virtuaaliympäristössä [60]*

SecureVieW varmistaa XenClient hypervisorin ja tunnistaa mahdollisen laitteen kokoonpanon peukaloinnin. SecureVieW käyttää TPM 2.0 määrittelyn mukaista ”sinetöintiä, engl. sealing” piirrettä varmistamaan, että salattu tietoaineisto on purettu ja avataan ainoastaan silloin kun ei ole epäilystä, että alustaa tai laitetta ei ole murrettu. Kun järjestelmä käynnistetään, eheyden tarkistus otetaan käyttöön ja tieto siitä tallennetaan alustan kokoonpanorekisteriin (Platform Configuration Register, PCR) TMP:ssä. TMP:n on

mahdollista määrätä salaamaan tietoaineisto ja sitomaan tietoaineiston purkaminen laitteen ehdolliseen tilaan siten, että salauksen purkaminen tehdään ainoastaan, jos PCR:ään tallennetut arvot vastaavat annettuja arvoja ja alusta on varmistettu eheäksi. Koska XenClient kokoonpanotiedostot on salattu ja salausavain on ”sinetöity” TMP:n PCR:ssä, hypervisor käynnistetään ainoastaan, jos PCR arvot täsmäävät järjestelmän odotettuihin arvoihin (Shpantzer 2013).

TPM on mikrosiru, joka on suunniteltu mahdollistamaan perustietoturvatoiminnot, ensisijaisesti sisältäen salausavaimet. TPM on yleisesti asennettu tietokoneen emolevylle ja kommunikoi tietokonejärjestelmän kanssa hyödyntämällä tietokoneen muistiväyliä. Tietokoneissa, joissa on tuettuna TPM-teknologia, on kyky luoda salausavaimia ja salata niillä joten salaus voidaan purkaa ainoastaan TPM-teknologialla. Tätä prosessia kutsutaan usein avaimen käärimiseksi (wrapping key) tai sitomiseksi (binding key), joka auttaa suojaamaan avaimen paljastumista. Jokaisella TPM:llä on juuriavain, jota kutsutaan muistijuuriavaimeksi (Storage Root Key), joka on tallennettu itse TPM:ään. Avaimen yksityinen osa luodaan TPM:ssä, joka ei koskaan näy muille tietokoneen komponenteille, ohjelmistoille, prosesseille tai henkilölle (Microsoft 2014).

Tietokoneet, joissa on tuettuna TPM-teknologia, voidaan luoda avain, joka ei ole ainoastaan käärittynä (wrapping) mutta on myös sidottuna (binding) tiettyihin alusta tarkistuksiin. Tämän tyyppinen avain voi olla käärimätön ainoastaan silloin kun tietokonealustan tarkistuksilla on sama arvot kuin niillä oli kun avain luotiin. Tätä prosessia kutsutaan avaimen sinetöimiseksi (sealing) TPM:ssä. Sinetöidyllä avaimella ja ohjelmistolla kuten Windows BitLocker Drive salauksella voidaan tietoaineisto lukita kunnes määritellyt laite- tai ohjelmistotason vaatimukset on saavutettu (Microsoft 2014).

TPM-teknologiassa yksityinen avain pidetään erillään käyttöjärjestelmän kontrolloimasta muistista. Avaimet voidaan sinetöidä TPM:ään ja tietyillä järjestelmän tilan tarkistuksilla – joka määrittelee sen luotettavuuden – voidaan tehdä ennen kuin avaimet ovat sinetöimättömiä ja vapautettu käyttöön. Koska TPM käyttää sen omaa sisäistä firmwarea ja loogisia piiriä käskyjen prosessoinnissa, se ei luota käyttöjärjestelmään ja eikä näin altistu ulkoisille ohjelmistohaavoittuvuuksille (Microsoft 2014).

TMP-teknologian lisäksi piirivalmistajat ovat kehittäneet myös Trusted Excecution Enviroment (TEE) -teknologiaa älypuhelimien kuten esimerkiksi Android, Symbian Os ja Windows Phone tietoturvan parantamiseksi. TEE luo älypuhelimen prosessoriin turva-alueen, jossa voidaan ajaa sovelluksia suojaamalla niitä viruksilta, haittaohjelmilta ja hyökkäyksiltä sekä mahdollistaa käsittelemään tietoaineistoa turvallisesti varmistamalla tietoaineiston luottamuksellisuuden ja eheyden (GlobalPlatForm 2015).

Tietoturvaa voidaan parantaa edelleen älypuhelimessa hyödyntämällä Secure Element (SE) -teknologiaa yhdessä TEE-teknologian kanssa. SE muodostuu ohjelmistosta sekä hyökkäyksen kestävästä laitteistosta. SE:tä voidaan hyödyntää älypuhelimessa kun käsitellään maksusovelluksia tai sähköistä allekirjoitusta (GlobalPlatForm 2015).

5.2 Tietoaineiston suojaukseen liittyviä tietoturvaratkaisuja

Luottamuksellisen tietoaineiston ja tietosuojan varmistamiseksi on kehitetty erilaisia kaupallisia tietoturvaratkaisuja suojaamaan kuluttajien ja organisaatioiden tietoaineistoja ja yksityisyyden suojaa pilvipalveluissa. Tietoaineiston salaustekniikoiden alalajien kuten homomorfinen salaus on kehitetty erilaisia versioita tietoaineiston salaamiseksi pilvessä siten, että tietoaineiston salausta ei tarvitse purkaa kun tietoaineistoa luetaan pilvessä (katso luku 4.3). Myös salausavainten jakamiseksi on kehitetty salaustekniikoita siten, että kolmannen osapuolen tekemä auditointi voidaan tehdä turvallisesti tietoaineiston paljastumatta.

Seuraavissa luvuissa 5.2.1 ja 5.2.2 on käsitelty kahta maailmanlaajuisesti johtavaa yhdysvaltalaisen tietoturvayrityksen tietoturvaratkaisua arkaluonteisen tietoaineiston luottamuksellisuuden säilyttämiseksi käytettäessä pilvipalveluita.

Pilvipalvelun IaaS, SaaS- tai PaaS-palveluja tarjoavat pilvipalvelun tuottajat voivat tarjota organisaatioille parempaa tietoturvaa ja tietosuojaa tarjoamalla pilvi-infrastruktuurin päällä esimerkiksi seuraavia tietoturvapalveluita.

5.2.1 Yhdysvaltalainen tietoturvayritys SafeNet

SafeNet (2014) on vuonna 1983 perustettu yhdysvaltalainen tietoturvaratkaisuja yrityksille tuottava maailman kolmanneksi suurin alan toimija. Tietoturvayritys omistaa 100 salausteknologiaa koskevaa patenttia yhdysvalloissa, joista 70 on patentoitu myös muissa maissa ympäri maailman. Se on myös eri standardointi järjestöjen jäsen kuten IEEE, IETF ja 3GPP. Yrityksen toiminta on keskittynyt muun muassa pilvipalveluissa erityisesti arkaluontoisen tietoaineiston suojaamiseen kuten käyttäjien ja sovellusten identiteetin suojaamiseen, kriittisten tapahtumien suojaaminen digitaalisissa prosesseissa, tietoaineiston salaaminen kun se luodaan, haetaan, siirretään, jaetaan ja tallennetaan.

SafeNet Cloud Security tuotevalikoimaan sisältyy kokonainen tietoturvaratkaisujen ekosysteemi, joka yhdistää jatkuvan suojauksen, joustavan salauksen, identiteetin suojan ja turvallisen viestinnän. Seuraavassa kuvataan lyhyesti SafeNetin arkaluonteisen tietoaineiston käsittelyyn liittyviä tietoturvaratkaisuja kuten virtuaaliympäristön suojaus (ProtectV), salausavainten suojaus (KeySecure), tiedostojen suojaus (Protect File), tietokannan suojaus (Protect DB).

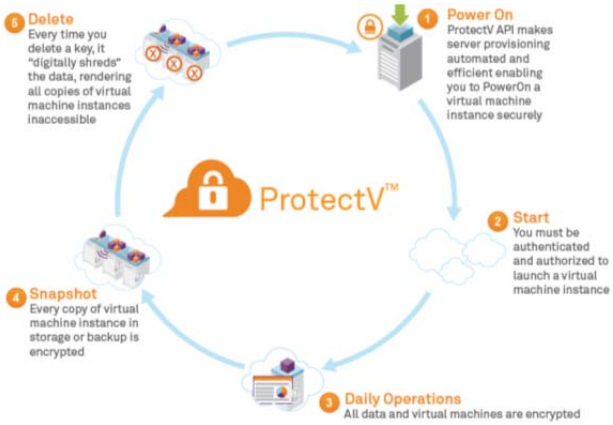
Virtuaaliympäristön suojaus mahdollistaa yhdistämään salauksen ja pilviympäristön avainten hallinnan siirrettäessä tietoaineistoa pilveen muun muassa:

- fyysiset palvelimet on suojattu samoilla tietoturvapoliitikoilla kuin virtuaalilaitteet (Virtual Machine, VM)
- koko virtuaalilaite (VM), instanssit ja muistit salataan, varmistetaan ja otetaan snapshotit (tietyn hetken ohjelmiston tila ajassa taaksepäin). Katso kuva 13.
- erotetaan ylläpitäjän salaus ja avainten hallinta hypervisorin ja muistilaitteiden ylläpidosta toisin sanoen eliminoidaan ylläpitäjän pääsy arkaluonteiseen tietoaineistoon
- tietovuodon sattuessa arkaluonteinen tietoaineisto käännettään nopeasti lukukelvottomaksi.

Virtuaaliympäristön suojauksella voidaan suojata ohjelmoitavia sovellusrajapintoja (Application Program Interface, API) virtuaalipalvelimien automaatiossa ja integraati-

ossa sekä esimerkiksi skriptauksessa komentokehote-editoreita (Command Line Interface, CLI). Katso kuva 15.

SafeNet lupaa, että koko virtuaalilaite ja kaikki sen kannat salataan salausratkaisulla, joka noudattaa muun muassa PCI DSS, SOX, HIPAA ja HITECH standardeja. Palveluun pääsee kiinni ainoastaan virtuaaliympäristön suojauksen StartGuard:lla, jolla hoidetaan käyttäjän valtuutus ja käyttöoikeuksien rajaaminen. Katso kuva 13.



Kuva 13. *Virtuaaliympäristön salausratkaisun elinkaaren vaiheet (SafeNet 2014).*

Kuvassa 14 on listattu virtuaaliympäristön suojauksen tukemat käyttöjärjestelmäalustat Amazon Web Services- ja VMware-virtuaaliympäristöissä.

Tarkemmin virtuaaliympäristö suojaa seuraavia pilvipalvelualustoja:

- Amazon Web Services (AWS) Marketplace
- Amazon Elastic Compute Cloud
- Amazon Virtual Private Cloud
- VMware vSphere

Operating System / Platform	AWS	VMware	Physical
Microsoft Windows Server 2003 R2 (64-bit), SP2	Yes	Yes	Yes
Microsoft Windows Server 2008 (64-bit), SP2	Yes	Yes	Yes
Microsoft Windows Server 2008 R2 (64-bit), SP1	Yes	Yes	Yes
Microsoft Windows Server 2012 (64-bit)	Yes	Yes	Yes
Microsoft Windows Server 2012 R2 (64-bit)	Yes	Yes	Yes
CentOS Linux 6.2 (64-bit)	Yes	No	No
CentOS Linux 6.4 (64-bit)	Yes	No	No
CentOS Linux 6.5 (64-bit)	Yes	No	No
SUSE Linux Enterprise Server (SLES) 10 SP4, 64-bit	No	Yes	No
SUSE Linux Enterprise Server (SLES) 11 SP1, 64-bit	No	Yes	No
SUSE Linux Enterprise Server (SLES) 11 SP3, 64-bit (FIPS is not available)	Yes	Yes	No
Red Hat Enterprise Linux (RHEL) 5.8, 64-bit	Yes	Yes	No
Red Hat Enterprise Linux (RHEL) 6.2, 64-bit	Yes	Yes	No
Red Hat Enterprise Linux (RHEL) 6.3, 64-bit	Yes	Yes	No
Red Hat Enterprise Linux (RHEL) 6.4, 64-bit	Yes	Yes	No
Red Hat Enterprise Linux (RHEL) 6.5, 64-bit	Yes	Yes	No
Ubuntu 12.04 LTS (FIPS is not available)	Yes	Yes	No
Ubuntu 14.04 LTS (FIPS is not available)	Yes	Yes	No

Kuva 14. *Tuetut käyttöjärjestelmät AWS- ja VMware-virtuaaliympäristöissä (SafeNet 2014)*

Salausavainten suojaus on keskitetty avaintenhallinta-alusta, joka on saatavilla fyysisenä laitteena tai kovennettuna virtuaalilaitteena. SafeNet avaintenhallinta laitteet noudattavat Federal Information Processing Standards (FIPS) tietoturvastandardeja. Kuvassa 15 on kuvattu salausavainten suojauksen tukemia teknologioita esimerkiksi algoritmeille.

Supported Technologies (All Models):	
API Support	KMIP 1.1, PKCS #11, JCE, MS-CAPI, ICAPI, and.NET
Network Management	SNMP v1, v2c, and v3 SNMP (v1, v2, and v3), NTP, URL health check, signed secure logs & syslog, automatic log rotation, secured encryption and integrity checked backups and upgrades, extensive statistics
Authentication	LDAP and Active Directory
Management Interfaces	**KeySecure Management Console:** Graphical user interface (GUI) available via web browser that is capable of high-grade 128-bit encryption. JavaScript must be enabled to access all functionality available through the management console. **Command Line Interface (CLI):** Command line interface (CLI) available over SSH or directly through the serial console port
Auditing and Logging	Cryptographically signed tracking of granular events. Configurable audit trail with local and remote (syslog) logging.
Supported Algorithms	The KeySecure supports the following public algorithms: → AES → ARIA → DES → DESede → HMAC-SHA1 → HMAC-SHA256 → HMAC-SHA384 → HMAC-SHA512 → RC4 → RSA → SEED
Operating System	Highly customized, hardened OS

Kuva 15. *Salausavainten suojauksen tukemat salausteknologiat (SafeNet 2014).*

Tiedostojen suojaus salaa täysin automaattisesti arkaluonteisen tietoaineiston verkkolevyillä ja tiedostopalvelimilla, joka mahdollistaa myös salaamaan ainoastaan tietyt tiedostot ja kansiot sekä kontrolloimaan kenellä on pääsy tiedostoihin. Salausavaimia hallinnoidaan salausavainten suojaus-ohjelmistolla yhdestä keskitetystä paikasta. Tiedostojen suojaus salaa AES:lla tietoaineiston siten, että se on suojattu läpi koko sen elinkaaren. Kuvassa 16 on eritelty tiedostojen suojauksen tukemia ominaisuuksia.

FILE ENCRYPTION SPECIFICATIONS	
Servers	A file server, web server, application server, database server, or other machine running compatible software
Network Shares	SMB/CIFS, NFS
Installation	Remote silent installation for easy deployment in any size environment
File Encryption Algorithm	AES
Supported Platforms	→ Apache Hadoop → Linux: Red Hat Enterprise, Oracle Unbreakable Enterprise Kernel, Suse → Microsoft Windows

Kuva 16. *Tiedostojen suojaus: tiedostojen salaaminen ja suojaaminen (SafeNet 2014).*

Tietokantojen suojaus salaa tietoaineiston, joka on tallennettu tietokantaan datakeskuksissa ja pilvessä. Tietokantojen suojaus mahdollistaa salaamaan tietoaineiston tietokannassa tiedosto- ja saraketasolla. Kuvassa 17 on tuettujen tietokantojen tekninen erittely.

Yhdistämällä tietokantojen suojauksen yhdessä SafeNet Cloud Security tietoturvaratkaisun kanssa, organisaatiot voivat varmistaa, että salattu tietoaineisto jää myös salatuksi sen koko elinkaaren ajaksi mahdollistaen kuitenkin valtuutettujen käyttäjien ja prosessien purkaa salaus kun on siihen tarvetta. Elinkaarisuojaus kasvattaa tietokantojen tietoturvaa ja helpottaa yhteistyötä eliminoimalla haavoittuvuudet tietokannan ulkopuolelta.

Monet tietoturvaa sääntelevät vaatimukset vaativat erottamaan tietoturvaan liittyvän ylläpidon tietokantojen ylläpidosta niin sanotulta ”super-käyttäjän” syntymisen riskiltä. Tietokantojen suojaus mahdollistaa tietoturvapolitiikan, jolla voidaan estää yksittäisen ylläpitäjän tekemästä kriittisiä konfiguraatio muutoksia ilman toisten ylläpitäjien oikeuksien myöntämistä.

SafeNet mahdollistaa keskitetysti hallinnoimaan salausjärjestelmää organisaatiossa, kattaen erilaiset web-sovellukset, sovelluspalvelimet, tietokannat, tiedostopalvelimet, ar-

kistoinnin ja virtuaaliympäristöt, tarjoten korkean luottamuksen avainten hallintajärjestelmän, jolla voidaan hallinnoida kaikki avaimet, joita käytetään salaukseen.

TECHNICAL SPECIFICATIONS	
Databases Supported	→ Oracle → Microsoft SQL Server → IBM DB2
Database Encryption Algorithms	→ AES → 3DES → DES → RSA (signatures and encryption) → RC4 → SHA-I → ACSHA-I
Supported Platforms	→ Microsoft Windows → Linux → UNIX

Kuva 17. *Tietokantojen suojauksen tekninen erittely (SafeNet 2014).*

SafeNet Cloud Security tietoturvaratkaisu keskittää salausprosessin, tietoturvapolitiikat ja avainten hallinnan yhdelle alustalle, joka on FIPS-validoitu fyysinen alusta tai kovennettu virtuaalinen tietoturvalaite, joka mahdollistaa joustavasti ylläpitämään fyysisiä ja virtuaalisia infrastruktuureja ja pilvipalvelun tuottajan ympäristöjä.

Tietoturvaratkaisu mahdollistaa seuraavia tietoturvaa parantavia asioita:

Sovellustason suojaus:

- Suojaa sovelluksia useamman toimittajan infrastruktuurin toimittamissa datakeskuksissa ja pilvessä
- Varmistaa tietoaineiston eheyden ja luottamuksellisuuden sähköisellä allekirjoituksella ja varmennuksella
- Ainoastaan valtuutetut käyttäjät saavat pääsyn tietoaineistoon.

Tiedostotason suojaus:

- Suojaa tietoaineistoa tiedostopalvelimilla ja jaettaessa tietoaineistoa verkossa

- Suorittamaan salauksen roolipohjaisesti, jolloin valtuuttamattomat käyttäjät ja prosessit eivät pääse kiinni tietoaineistoon
- Voidaan ottaa käyttöön verkkojaoissa, tiedostopalvelimilla, web-palvelimilla, sovelluspalvelimilla, tietokannoissa tai muissa laitteissa, joissa ajetaan Linux yhteensopivia ohjelmistoja.

Transparentti-tietokannan salaus:

- Transparentti-sovellus, sarake-tason tietokantasalaus useamman toimittajan toimittamissa tietokantajärjestelmissä joita käytetään datakeskuksissa ja pilvessä
- Keskitetty tietoaineiston pääsynvalvonta on tehty roolipohjaisella rajoitusvaihtoehdoilla ja säännöllisellä avainkierrolla.

Virtuaalisen kuorman salaus (prosessien määrä, joka on annettu suorittimelle käsiteltäväksi annetussa ajassa):

- Täydellinen virtuaalilaitteiden instanssien ja muistilaitteiden salaus. Salaamatonta tietoaineistoa ei kirjoiteta levylle.
- Tuki AWS Marketplace ja WMware ympäristöille
- Todentamisen esikäynnistys varmistaa, että ainoastaan valtuutetut käyttäjät pääsevät kiinni tietoaineistoon

5.2.2 Yhdysvaltalainen tietoturvayritys Trend Micro

Trend Micro on perustettu vuonna 1988 yhdysvalloissa. Trend Micron SecureCloud tietoturvaratkaisu toimittaa tietoaineiston suojausta pilvi- ja virtuaaliympäristöihin salauksella ja politiikka pohjaisella avaintenhallinnalla sekä uniikilla palvelimen kelpuutus ratkaisulla. Trend Micron tietoturvaratkaisuja käyttävät johtavat pilvipalvelun tuottajat kuten Amazon Web Service ja WMware vCloud Air tai virtuaaliympäristöissä kuten VMware ja CloudStack.

Trend Micro (2014) mahdollistaa tehokkaan ja helppokäyttöisen salauspalvelun pitämään tietoaineiston suojattuna niin julkisissa kuin yksityisissä pilvissä sekä VMware vSphere virtuaaliympäristöissä.

Seuraavassa on kuvattu tietoturvaratkaisun peruskomponentit: Runtime Agent, Management Server ja VMware vCloud API (katso kuva 18).

Runtime Agent:

Runtime Agent on ohjelmistomoduuli, joka on asennettu virtuaalikoneen imagelle pilvipalvelun tuottajan ympäristössä. Runtime Agent mahdollistaa eheyden tarkistus toiminnallisuuden kuten IP-osoite ja sijainti. Tietoturvaratkaisu hyödyntää AES-salausta taltioiden salauksessa käyttäen VM-tason salausta. Kokokoonpanonhallintatyökalu sijaitsee pilvipalvelun tuottajan ympäristössä osana Runtime Agentia. Runtime Agentin asennuksen jälkeen voidaan aktivoida kokokoonpanonhallintatyökalu hyödyntämällä asennusvelhoa.

Kokoonpanonhallintatyökalu mahdollistaa seuraavat:

- Pilvipalvelun tuottaja ja virtuaalisointi laajennoksen
- Pilvipalvelun tuottajan valtuutukset
- Tietoturvaratkaisun käyttäjätilin ID
- Webservice API URL
- Laitetiedot ajettavasta laiteinstanssista
- Laitesalauksen

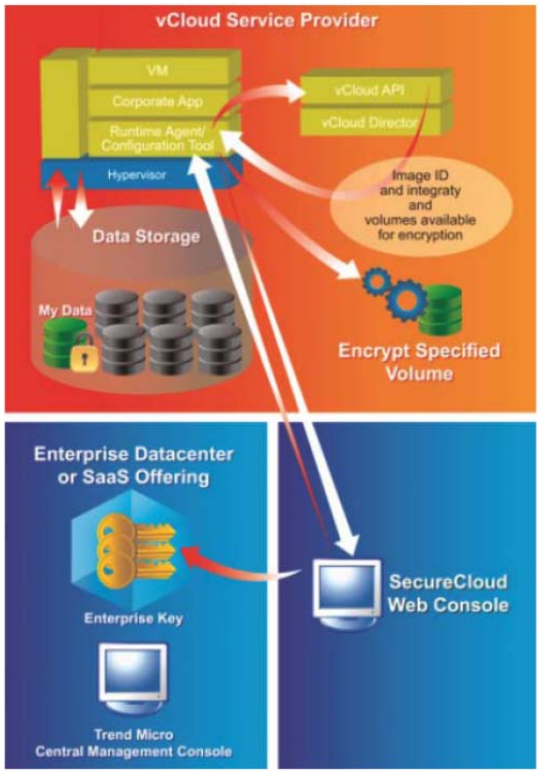
Management Server:

Trend Micro SecureCloud tietoturvaratkaisu tarjotaan useilla toimitusmalleilla, jota voidaan käyttää Trend Micron ylläpitämänä useamman asiakkaan palveluna tai asiakas voi ottaa käyttöön pilvipalvelussa oman tietoturvaratkaisun hallintapalvelimen. Hallintapalvelin ylläpitää avainten hyväksyntäprosessia, lokitusta ja raportointia. Ylläpitotoimenpi-

teet hallintakonsolilla (Central Management Console) perustuvat ylläpitäjien roolipohjaisiin käyttöoikeustasoihin.

VMware vCloud API:

vCloud API (katso kuva 18) rajapinnalla voidaan integroida asiakkaat, yhteistyökumppanit ja internet-ratkaisutoimittajat Trend Micro vCloud Director tuotteeseen. vCloud API käytetään tietoturvaratkaisussa päättelemään virtuaalilaitteen imagen identiteetti vCloud ympäristössä. vCloud API käytetään myös tunnistamaan mitä muistilaitteitta vCloud-ympäristössä on saatavilla salausta varten.



Kuva 18. *Tietoturvayritys B:n tietoturvaratkaisun peruskomponentit (Trend Micro 2014).*

Runtime Agent (katso kuva 18) käyttää vCloud API rajapintaa tunnistamaan vCloud virtuaalilaiteiden imagen identiteetin ja eheyden. Tämä tieto on haettu vCloud APIsta ja lähetetty hallintapalvelimelle, jossa käyttäjälle joko valtuutetaan tai kielletään salausavaimen käyttö pyydettyyn virtuaalilaitteen imageen, perustuen valtuutetun vCloud virtuaalilaitteen imagen identiteettiin ja eheyteen.

Runtime Agentin kokoonpanonhallintatyökalu kerää tietoa siitä mitä datan tallennuslaitteita on saatavilla salausta varten.

Kuvassa 19 on kuvattu tietoturvaratkaisun VMware-ratkaisun tietoturvapiirteet kuten uhkilta suojautuminen, pääsynvalvonta ja yksityisyys. Tietosuojan näkökulmasta voidaan huomioida, että Trend Micron tietoturvaratkaisu varmistaa, että virtuaali- ja muistilaitteiden muisteihin tallennettu tietoaineisto on salattuna koko ajan.

vSphere and vCloud API Protection & Control	
Threat Protection	▪ Checks existence of Trend Micro security software providing intrusion detection and prevention, firewall, integrity monitoring, log inspection, and anti-malware capabilities. ▪ Ensures privacy amongst tenants by creating segregation through encryption. ▪ Provides the ability to adhere to compliance regulations by separation of duties. ▪ Uses industry proven AES encryption of the data to provide a robust data loss protection solution, securing intellectual property.
Access Control	▪ Uses identity- and integrity-based policy enforcement to ensure only authorized virtual machines receive encryption keys. ▪ Enforces separation of duties with role-based management. ▪ Provides access to management console supported by major authentication standards, including Microsoft Active Directory, SAML 2.0, and leading identity and access management systems.
Privacy	▪ Protects communication between Agent and Key Manager via AES 256 session keys. ▪ Does not store cloud provider credentials. ▪ Ensures data at rest remains encrypted at all times. ▪ Protects residual data remaining on physical servers after volumes are vacated or hardware is retired.
vSphere and vCloud API Abstraction & Management	
API Lifecycle	▪ Uses the Web UI to reflect the vCloud inventory, providing intuitive encrypted vCloud Disk management. ▪ Automatically supports API versioning, including rollback to previous version.
Orchestration	▪ Bases policy-driven API control on environment metadata. ▪ Controls storage availability based on environment integrity with user-defined policies. ▪ Supports vCloud Director 1.0 & 1.5 and vSphere, allowing for control of sensitive information throughout the virtualized infrastructure. ▪ Leverages vCloud's built in multi-tenancy to isolate customer data and session.
Protocols supported	▪ Makes all API calls over HTTPS. Key Management API interfaces are only available over HTTPS.
High Availability	▪ Architected as a horizontally scalable solution offering multiple front-end Key Managers.
Management API	▪ Uses Management API to allow customers to integrate the solution into their customer facing portals, creating an intuitive customer experience.
Standards	
Supported standards	▪ Includes SAML 2.0, REST, Microsoft Active Directory, XML 1.0

Kuva 19. *VMware ratkaisun tietoturvapiirteet (Trend Micro 2014).*

Trend Micro (2014) tarjoaa politiikka ohjautuvan avaintenhallintajärjestelmän (katso kuva 19) siten, että käyttäjä voi itse päättää missä ja koska salattuun tietoaineistoon voidaan päästä kiinni. Sen lisäksi identiteettiin ja eheyteen liittyviä sääntöjä sovelletaan kun palvelut pyytävät pääsyä suojattuihin muistitaltioihin. Koska tietoturva pilvessä on jaettu vastuullisuus, on erittäin tärkeää, että tiedetään täsmälleen mistä ollaan vastuussa.

Pilvipalvelun tuottajat tyypillisesti kattavat fyysisen ja verkko infrastruktuurin ja virtuaalitason tietoturvan mutta pilvipalvelun käyttäjän vastuulle jää turvata käyttöjärjestelmän, sovellusten ja tietoaineiston tietoturva. Tietoturvaratkaisu lupaa suojata arkaluontoisen tiedon varkauksilta, paljastumiselta tai tietoaineiston hyväksymättömältä siirrolta toisen maan datakeskukseen.

Trend Micron (2014) mukaan tietoturvaratkaisu käyttää VM-tason salausta, joka mahdollistaa salaaman tietoaineiston virtuaalilaitteen työmuistissa käytettäessä eri avaimia kuhunkin pilvipalvelun käyttäjän tietoon. Käyttäjän vaihtaessa pilvipalvelun tuottajaa säilyy työ- ja levymuisteissa oleva data edelleen salattuna.

Trend Micron SecureCloud tietoturvaratkaisun politiikkapohjainen avainten hallinta ja pääsynvalvonta mekanismi mahdollistavat käyttäjän määrittelemään millä palvelimilla pilvessä on oikeus käyttäjän suojattuun dataan. Käyttäjän pilviympäristössä ajettavien virtuaalipalvelimien tulee siten ensin autentikoitua tietoturvaratkaisun avainten hallintapalvelimella käyttämällä valtuuksia, jotka on salattu VM:n kernelissä. Määriteltyihin poliitikoihin perustuen avainten hallintapalvelimelle toimitettu tieto on siten tarkistettu ja pilviympäristö todettu turvalliseksi vapauttamaan salausavaimia. Tietoturvaratkaisun politiikkapohjainen avainten hallinta mahdollistaa määrittelemään ylläpitäjien oikeudet pilvipalvelimiin roolipohjaisesti esimerkiksi kaikki oikeudet, avainten hallinta tai pääsy ainoastaan lokitietoihin.

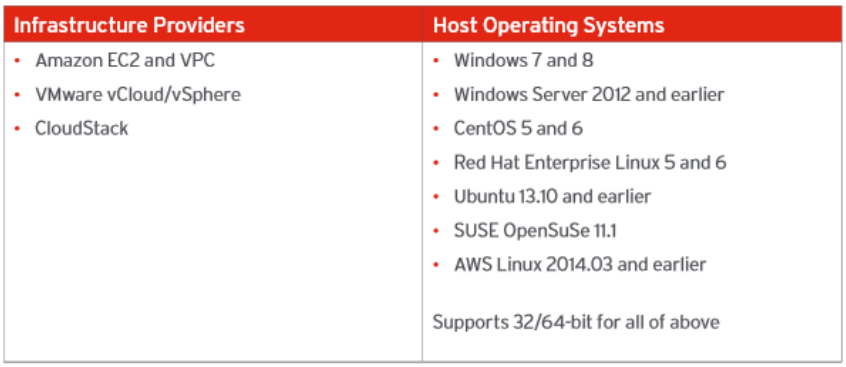
Tietoturvaratkaisu auttaa myös kontrolloimaan tietoaineistoon pääsyä eristämällä fyysisten muistilaitteiden avaimet pilvipalvelun tuottajalta. Tämä estää pilvipalvelun infrastruktuuria ylläpitäviltä pääsyn tietoaineistoihin tai avaimiin ja mahdollistaa siten pilvipalvelun asiakkaalle vapauden siirtää data yhdeltä palvelun tuottajalta toiselle ilman pelkoa datan lukkiutumisesta pilvipalveluun.

SecureCloud tietoturvaratkaisu mahdollistaa myös lokituksen ja raportoinnin kaikille toiminnoille, jotka on suoritettu järjestelmässä tai avainten myöntämisessä.

Tietoturvaratkaisu tukee muun muassa seuraavia lakeja ja standardeja arkaluonteisen tiedon käsittelyssä kuten Insurance Portability and Accountability Act (HIPAA), Health

Information Technology for Economic and Clinical Health Act (HITECH), Sarbanes-Oxley ja Payment Card Industry Data Security Standard (PCI DSS). Tietoturvaratkaisu tukee myös AES-256 lohkosalausta ja on FIPS 140-2 sertifioitu.

Tietoturvaratkaisu tukee seuraavia pilvipalvelu- ja käyttöjärjestelmä alustoja (kuva 20):



Infrastructure Providers	Host Operating Systems
• Amazon EC2 and VPC • VMware vCloud/vSphere • CloudStack	• Windows 7 and 8 • Windows Server 2012 and earlier • CentOS 5 and 6 • Red Hat Enterprise Linux 5 and 6 • Ubuntu 13.10 and earlier • SUSE OpenSuSe 11.1 • AWS Linux 2014.03 and earlier Supports 32/64-bit for all of above

Kuva 20. *Tietoturvaratkaisun tukemat virtuaaliympäristöt ja käyttöjärjestelmät (Trend Micro 2014).*

Trend Micro (2014) lupaa seuraavia ominaisuuksia arkaluonteisen tietoaineiston suojaamiseksi:

- Käyttäjä voi itse hallita salausavaimia
- Estää pilvipalvelun tuottajan pääsemästä kiinni tietoaineistoon
- Täysi tietoaineiston salaus, transparentti tietokantapalvelimille ja sovelluksille
- Keskitetty avaintenhallinta; politiikkapohjaisella avainten julkaisulla voidaan automatisoida koska ja missä tietoaineistoa voidaan käsitellä
- Avaimia pyydettäessä automaattisesti todennetaan palvelimen identiteetti ja eheys
- Varmistaa, että tietoaineisto ei ole haettavissa pilvessä sen jälkeen kun tietoaineisto on pysyvästi poistettu
- Käytetään identiteetti- ja eheyspohjaisia politiikoita valvomaan avainten ja tietoaineiston salausta
- Voidaan käyttää politiikoita valvomaan missä ja milloin tietoaineistoa on haettu
- Tietoaineisto voidaan salata ja avata pilven tallennuslaitteella siten, että se on koko ajan suojattuna

- Salaus ei vaikuta suorituskykyyn
- Käytetään rooli-pohjaista käyttöoikeuksien hallintaa tehtävien erottamiseksi
- Avainten julkaisun ja virtuaalilaitteiden valtuutuksen automatisointi nopeissa toiminnoissa
- Auditointia varten lokitus.

5.3 Tietoaineiston suojaukseen liittyvät ongelmat

Vaikka pilvipalvelun tuottajat voivat tarjota käyttäjille monia hyötyjä, kuitenkin tietoturvariskit esittävät suurta roolia pilviympäristöissä (Viega 2009). Mei *et al.* (2009) mukaan yksityisen ja tärkeän tiedon suojaaminen kuten luottokortti- tai potilastiedot hyökkääjiltä tai pahantahtoisilta tunkeutujilta on tärkeää. Siirtämällä tietokantoja suuriin datakeskuksiin, aiheuttaa tämä monia tietoturvahaasteita kuten virtuaalisoinnin haavoittuvuudet, saatavuus, yksityisyyden suoja, tiedon eheys, luottamuksellisuus, tiedon menetykset ja varastaminen. Eri pilvimalleissa tietoturvavastuut käyttäjien ja pilvipalvelun tuottajien välillä ovat erilaisia. Brunette *et al.* (2009) mukaan Amazonin EC2 pilvimallissa palveluntuottaja vastaa virtuaaliympäristön fyysisestä tietoturvasta kun taas pilvipalveluja käyttävän asiakkaan vastuulle jää vastata IT-järjestelmistä kuten käyttöjärjestelmästä, sovelluksista ja tietoaineistosta.

Tabaki *et al.* (2010) mukaan vastuunjako tietoturvasta jakaantuu käyttäjien ja pilvipalvelun tuottajien välillä riippuen valitusta käyttöönotto- ja pilvipalvelumallista. SaaS-palvelumallissa pilvipalvelun tuottaja on enemmän vastuussa sovellusten tietoturvasta kuin käyttäjät. PaaS-palvelumallissa pilvipalvelun tuottajan vastuulle kuuluu varmistaa, että käyttäjien rakentamat sovellukset on eristetty toisistaan. IaaS-palvelumallissa käyttäjät vastaavat käyttöjärjestelmien ja sovellusten tietoturvasta kun taas pilvipalvelun tuottaja tietoaineiston tietoturvasta. Ristenpart *et al*. (2009) mukaan julkisessa käyttöönottomallissa korostuu tietoturvan merkitys enemmän kuin yksityisessä mallissa koska vahingot, jotka tapahtuvat fyysiseen tietoturvaan tai sen hallintaan ja ylläpitoon aiheuttaa monia ongelmia. Myös koska pilvipalveluita käytetään yli julkisen tietoverkon (internet), aiheuttaa tämä tietoturvaongelmia myös pilvipalveluiden tietoturvaan riippumatta siitä miten hyvin pilvipalvelun tuottaja on suojannut pilvipalvelunsa.

Mohta *et al.* (2012) mukaan suojaamatonta tietoaineistoa ei voida tallentaa suoraan pilveen koska pilvipalvelun tuottajalla on suora pääsy tietoaineistoon ja siten tietoaineiston luottamuksellisuus menetetään. Myös pahantahtoinen pilvipalvelun ylläpitäjä voi muokata palvelun käyttäjän tietoaineistoa ja siten samalla menetetään myös tietoaineiston eheys. Tietoaineiston eheyden ja luottamuksellisuuden säilyttämiseksi tarvitaan salaustekniikoita tietoaineiston salaamiseksi. Luvussa 4 kuvataan joitakin salaustekniikoita tietoaineiston tallentamiseksi pilveen turvallisesti.

Pilvipalvelun käyttäjät voivat hyödyntää myös kolmannen osapuolen tarjoamia tietoturvapalveluita tietoaineiston eheyden ja luottamuksellisuuden varmistamiseksi. Tähän liittyy kuitenkin tietoturvaongelmia riippuen miten palvelu on toteutettu. Ongelmaksi muodostuu, miten varmistaa kolmannen osapuolen luotettavuus muun muassa tietoaineiston luottamuksellisuus ja ettei tietoaineistoa siirretään edelleen eteenpäin (Mohta *et al.* 2012).

Tavallisesti salaukseen käytettävät avaimet tallennetaan käyttäjän tietokoneen levylle, jotka salataan käyttäjän julkisella avaimella. Salattu avain puretaan käyttäjän salaisella avaimella. Salausjärjestelmä toimii hyvin kun käytetään henkilökohtaisia tietokoneita salaukseen. Sen sijaan, jos käytetään kolmatta osapuolta salauksessa kuten pilvipalvelun tuottajaa, on olemassa tietovuodon mahdollisuus. Tämä sen vuoksi, että salausavaimet tallennetaan levylle ja salauksessa käytetään pilvipalvelun tuottajan julkista avainta ja pilvipalvelun tuottajan ylläpitäjällä on suurimmat oikeudet pilven tallennustilaan. Siten pilven ylläpitäjä voi helposti päästä kiinni salaus- ja purkausavaimiin ja siten purkaa ja muokata käyttäjän tietoaineistoa. Luonnollisesti tällöin menetetään sekä luottamuksellisuus ja eheys käyttäjän pilveen tallentamaan tietoaineistoon. Tämän tietoturvaongelman välttämiseksi tarvitaan pilvipalvelun käyttäjän ja sen tuottajan välille tietoturvallinen luottamussuhde. Tämä saavuttamiseksi tarvitaan tietoturvaratkaisu, joka takaa käyttäjän pilveen tallentaman tietoaineiston luottamuksellisuuden ja eheyden. Luvussa 5.2 on kuvattu kaksi tietoturvaratkaisua tämän saavuttamiseksi.

5.4 Yhteenveto

SafeNet Cloud Security tietoturvaratkaisu lupaa säilyttää tietoaineiston luottamuksellisuuden pilvessä erottamalla salauksen ja avainten hallinnan hypervisorin ja muistilaitteiden ylläpidosta. Myös tietovuodon tapahtuessa voidaan arkaluonteinen tietoaineisto kääntää lukukelvottomaksi. SafeNetin www-sivuilla ei kuitenkaan selvinnyt miten tämä käytännössä tehdään koska jos tietoaineisto on jo paljastunut, on tietoaineiston lukukelvottomaksi saattaminen myöhässä.

Trend Micron SecureCloud tietoturvaratkaisussa tietoaineisto on pilven muistilaitteilla koko ajan salattuna. Myös pilvipalvelun käyttäjä hallitsee itse salausavaimia sekä käytetään identiteetti- ja eheyspohjaisia politiikoita valvomaan avainten ja tietoaineiston salausta.

6 CASE-TUTKIMUS PILVIPALVELUJEN TIETOSUOJAN VARMISTAMISESTA

Tuloksia on käsitelty kolmen case-tapauksen A, B ja C pohjalta arvioimalle heidän www-sivujen materiaalia ja vertaamalla tietoja kyselytutkimuksen kysymyksiin vastauksien saamiseksi. Kaikkiin tietosuojaa koskeviin kysymyksiin ei voida päätellä vastausta julkisten www-sivujen materiaalin pohjalta.

Seuraavissa luvuissa 6.1 – 6.3 on kuvattu ja analysoitu kolmen tyypillisen suomalaisen pilvipalvelun tuottajan A, B ja C tietoturvaratkaisuja suojata pilvipalvelua luvattomalta käytöltä. Tietosuojan varmistamiseen liittyvää tietoturvaa arvioidaan sovellustietoturvan, datan suojauksen, salausavainten hallinnan, pääsynvalvonnan, lokien valvonnan, tunkeutumisen estämisen, tietoturva-standardien noudattamisen ja vaatimustenmukaisuuden näkökulmasta. Käsiteltävien pilvipalveluiden tuottajien anonymiteetin säilyttämiseksi yrityksiä tai heidän tuotteittaan ei mainita nimeltä vaan käsitellään tapauksina A, B ja C.

6.1 Suomalainen pilvipalvelun tuottaja A

Pilvipalvelun tuottaja A julkaisi vuonna 2013 uuden lähinnä kuluttajille suunnatun pilvipalvelun, jossa voidaan tallentaa muun muassa musiikkia, valokuvia, dokumentteja henkilökohtaiseen pilveen ja tuoda myös Facebookista ja Dropboxista jo tallennetut kuvat samaan paikkaan. Tämän lisäksi on erikseen yrityksille suunnattu pilvipalvelu, joka on tehty yritysten yhteistyötä ja tietosuojaa varten. Pilvipalvelutuottaja A:n datakeskukset sijaitsevat Suomessa, siten tietoaineiston tietosuojaa koskee Suomen lainsäädäntö.

Pilvipalvelun tuottaja A:n mukaan pilvipalveluun tallennetut ja sieltä jaetut yrityksen asiakirjat ja mediatiedostot ovat yhdessä turvallisessa paikassa ja yritykset ja heidän kumppanit voivat tehdä yhteistyötä synkronoidusti. Pilvipalvelun tuottaja A lupaa myös, että heidän tuottaman pilvipalvelun avulla voidaan jakaa sisältöä helposti ja turvallisesti haluamilleen tahoille.

Pilvipalvelun avulla voi liittää tiedostoja eri pilvipalveluista ja laitteista yhteen turvalliseen paikkaan. Pilvipalveluita voi käyttää sekä online- että offline-tilassa, kaikilla laitteilla. Palvelu mahdollistaa jakamaan sisältöä valittujen ihmisten kanssa.

Pilvipalvelussa asiakkaiden tietietoaineisto salataan automaattisesti käyttämällä AES-256 salausalgoritmia sekä tiedonsiirrossa että tallennettaessa tietoaineistoa pilven tallennuslaitteille. Käyttäjien tietoaineisto on myös eristetty toisistaan palvelussa. Pilvipalvelu tuottaja A:n mukaan palvelun useimmat järjestelmäkomponentit on toteutettu ohjelmointikielillä, jotka kestävät tavallisimmat ohjelmistohaavoittuvuudet. Esimerkiksi tietokantahaut on suojattu käyttämällä parametrisoituja proseduureja, joihin on rajoitetut tietokantatilit. Pilvipalvelu tuottaja A:n mukaan tämä vaikeuttaa merkittävästi hyökkääjän pääsyä tietokantaan ja tietoaineistoon.

Pilvipalvelussa ylläpitäjillä on rajoitetut ylläpito-oikeudet pilvipalvelussa ja ylläpitäjillä ei ole pääsyä asiakkaiden tietoaineistoihin muun muassa henkilökunnan taustat selvitetään ennen oikeuksien myöntämistä. Ylläpitäjien tulee suorittaa asianmukainen ylläpitokoulutus ennen kuin ylläpito-oikeuksia palveluun myönnetään, muun muassa varmistetaan, että ylläpitäjä osaa ja tuntee tietoturvalliset menettelytavat.

Pilvipalvelun tuottaja A teettää säännöllisesti kolmannen osapuolen tekemiä tietoturva-auditointeja pilvipalveluun. Se myös monitoroi jatkuvasti kolmannen osapuolen komponentteja (käyttöjärjestelmät, web-palvelimet, tietokannat) mahdollisilta ilmoituksista tietoturvahaavoittuvuuksista ja -korjauksista. Pilvipalvelua monitoroidaan ja kerätään lokitietoa jatkuvasti esimerkiksi luvatonta pääsyä vastaan. Valvonnassa käytetään muun muassa tunkeutumisenestojärjestelmää. Pilvipalvelun valvontaohjelma antaa välittömästi varoituksia ja hälytyksiä ylläpitäjälle, jos joitain poikkeavaa on menossa esimerkiksi jos tarvitaan huoltotoimenpiteitä tai tulee lisätä resursseja palvelussa tai ulkoisesta uhasta.

Pilvipalvelussa kaikki tietoaineisto skannataan viruksien varalta. Pilvipalvelun arkkitehtuurissa kaikki tietoliikenne skannataan erilisissä ”hietalaatikoissa” ennen tietoaineiston tallentamista pilvipalveluun näin palvelussa voidaan tehokkaasti suojata järjestelmän komponentteja ja käyttäjän tietoaineistoa viruksilta.

Pilvipalvelun tuottaja A:n mukaan pilvipalvelun saatavuus on varmistettu suunnittelemalla kaikki huoltotoimenpiteet huolellisesti ennakkoon. Kaikki hätäkorjaukset tai muutokset järjestelmään tehdään siten, että itse pilvipalvelun toiminta ei katkea tai häiriinny. Huoltotoimenpiteiden yhteydessä saatetaan poistaa käytöstä myös vanha levypakka. Pilvipalvelun tuottaja A:n mukaan tallennuslevyillä oleva tietoaineisto poistetaan erityisen poisto-ohjelman avulla siten, että tietoa ei poiston jälkeen vuoda vääriin käsiin.

Pilvipalvelun tuottaja A:n tuottamat palvelut hyödyntävät kolmannen osapuolen datakeskuspalveluja. Datakeskuskusten fyysinen tietoturva on varmistettu muun muassa suojamuureilla, pääsynvalvonnalla ja valvonta- ja hälytysjärjestelmillä ehkäisemään ja suojaamaan luvattoman pääsyn datakeskukseen. Pilvipalvelun saatavuus on varmistettu myös kahdentamalla fyysisesti datakeskusten laitteet muun muassa redundantit voimalähteet ja tietoliikenneyhteydet. Datakeskuksia on suojattu myös luonnonkatastrofien varalta kuten tulvaa ja tulipaloa vastaan. Katastrofien varalta pilvipalvelun tuottaja A ylläpitää toipumissuunnitelmaa, jossa on kuvattu miten tulee toimia ja menetellä kriisitilanteessa.

Pilvipalvelu auttaa käyttäjää luomaan vahvan salasanan palveluun ja jos käyttäjä unohtaa salasanan, lähettää palvelu käyttäjän sähköpostiin resetointi-linkin, jossa käyttäjä voi itse resetoida salasanan. Pilvipalvelussa hyödynnetään 2-vaiheista autentikointia, jossa käytetään tietoturvakoodia ja koodia voi käyttää istunnon aikana vain kerran. Pilvipalvelun käyttäjän laitteeseen on asennettu sovellus, joka generoi joka minuutti uuden aikaperusteisen turva-koodin ja samoin tehdään pilvipalvelun autentikointipalvelimella. Tämä estää tehokkaasti krakkereita tunnistautumaan pilvipalveluun toisena käyttäjänä.

Saatavilla olevan materiaalin pohjalta pilvipalvelun tuottaja A ei kerro mitä standardeja kuten ISO/IEC 27001 tai suomalaisten viranomaisten ohjeita ja suosituksia muun muassa VAHTI- ja KATAKRI II –ohjeita he noudattavat varmistaakseen pilvipalvelun tietoturvan ja tietosuojan.

A:n pilvipalvelu lupaa seuraavia tietoturvapalveluja:

- Kaikki sisällöt tarkastetaan automaattisesti haittaohjelmien varalta
- Tietojen vahva salaus tiedonsiirron ja säilytyksen aikana
- Tiedot tallennetaan kahteen maantieteellisesti redundanttiin tietokonekeskukseen Suomessa
- Hallitse pilviäsi - hallitse, hae ja organisoi sisältöjä kaikissa käyttämissäsi eri pilvissä
- Tietosuoja yhdistettynä palkittuun tietoturvaan
- 2-vaiheinen autentikointi, jossa käytettään turvakoodia

Analyysi pilvipalvelun tuottaja A:sta:

Pilvipalvelun tuottajan A kuten myös B ja C ovat toteuttaneet infrastruktuuri- ja sovellustietoturvan suojaamiseksi tekniikkaa suojaamaan ja havaitsemaan ympäristössä tapahtuvat ulkoiset hyökkäys- ja tunkeutumisyritykset. Pilvipalvelun tuottaja A tekee myös sovellusten haavoittuvuus-skannauksia säännöllisesti. Myös voidaan päätellä, että pääsyä asiakkaan aineistoon yrityksen sisältä käsin on estetty ylläpitäjiltä ja tätä myös valvotaan keräämällä lokitietoa etuoikeudellisesta pääsystä tietoturvallisuuden hallintajärjestelmiin.

Toisin kuin pilvipalvelun tuottaja B ja C osalta saatavilla olevan materiaalin pohjalta ei kuitenkaan voida päätellä mitä virtuaaliteknologioita he hyödyntävät käyttämissään datakeskuksissa. Siten ei myöskään voida päätellä, että voidaanko A:n tarjoamassa pilvipalvelussa hyödyntää SafeNetin tai Trend Micron tietoturvaa parantavia ratkaisuja. Myöskään ei voida päätellä, että voidaanko hyödyntää IBM:n kehittämää Trusted Platform Module –teknologiaa parantamaan tietoturvaa pilvipalvelun alustoilla.

Pilvipalvelun tuottaja A tarjoaa myös asiakkailleen turvallisen suojatun tietoliikenneyhteyden AES-salauksella siirrettäessä ja tallennettaessa tietoaineistoa palveluun. Käytetystä symmetrisestä salausmenetelmästä voidaan päätellä, että asiakas hallinnoi itse salausavaimia ja niitä ei tallenneta pilvipalveluun.

Sen sijaan pilvipalvelun tuottajan A palvelun datan suojauksesta ja luokittelusta sekä datan elinkaarenhallinnasta ei voida käytetyn materiaalin pohjalta arvioida tietosuojan varmistamisen näkökulmasta mitään. Myöskään ei ole tietoa noudattaako pilvipalvelun tuottaja A suomalaisten viranomaisten suosituksia esimerkiksi VAHTI 3/2012, KATAKRI II suojaamaan yksityisyyttä ja tietoaineistoa pilvipalvelussa.

6.2 Suomalainen pilvipalvelun tuottaja B

Pilvipalvelun tuottaja B tarjoaa IaaS, SaaS ja PaaS pilvipalvelumalleihin perustuvia ratkaisuja. Esimerkiksi SaaS-palveluista yritys tarjoaa Microsoft Exchange sähköposti- ja kalenteripalveluja ja Microsoft Lync-viestintäratkaisun. IaaS-palvelussa tarjotaan kapasiteettipalveluja ja PaaS-palvelu tarjoaa valmiita avaimet käteen ratkaisuja, jossa asiakas voi itse hallita infrastruktuurin päällä olevia sovellusten- ja ohjelmistojen kehitystyökaluja.

Pilvipalvelun tuottaja B datakeskukset ja runkoverkko sijaitsevat Suomessa. Pilvipalvelun tuottaja B lupaa, että heidän palvelunsa tietoturva rakentuu useasta osakokonaisuudesta, kuten turvallisista tietoliikenneyhteyksistä, luotettavista palvelinkeskuksista, kehittyneistä ohjelmistoista sekä osaavasta henkilöstöstä. Pilvipalvelun tuottaja B:n tietoturvan hallinta pohjautuu ISO/IEC 27001, VAHTI sekä KATAKRI II parhaisiin käytäntöihin.

Pilvipalvelun tuottaja B:n pilvipalvelut täyttää palvelinkeskusten osalta myös PCI-DSS standardin vaatimukset, joka määrittelee korttimaksamisen tietoturvallisuuden tekniset vaatimukset sekä FICORA 54/2012M määräyksen viestintäverkkojen ja -palveluiden varmistamisesta. Pilvipalvelun tuottaja B palvelinkeskusten fyysinen suojaustaso täyttää muun muassa seuraavat vaatimukset:

- Palvelinkeskukset sijaitsevat Suomessa
- Kaikilla työntekijöillä on sanktioidut salassapitosopimukset
- Vähintään n+1 UPS, sähkönsyöttö ja jäähdytys
- Automaattinen varavoima diesel generaattoreilla
- 24/7 miehitetty konesali

- Tallentava videovalvonta
- Liikkeentunnistus
- Murtohälytysjärjestelmä
- Sammutusjärjestelmät
- Kaksi erillistä saatavuusaluetta, jotka ovat maantieteellisesti hajautettu toisistaan
- Täysin vikasietoinen runkoverkko

Pilvipalvelun tuottaja B:n tuottamat palvelut perustuvat avoimen lähdekoodin OpenStack -teknologiaan, jolla voidaan rakentaa IaaS-palveluja. OpenStack -pilviteknologia ei sido kuluttajaa ja voivat helposti vaihtaa halutessaan pilvipalvelun tuottajaa. Teknologiaa kehittää aktiivisesti 230 yritystä kansainvälisesti, jotka varmistavat jatkuvat tietoturvapäivitykset alustaan.

Avoimen lähdekoodin järjestelmä on testattu ja todettu luotettavaksi kymmenissä eri pilvialustoissa ympäri maailman. Asiakkaiden tietoaineistoa säilytetään Suomessa pilvipalvelun tuottaja B konesaleissa, ja itse pilvialusta on alusta loppuun pilvipalvelun tuottaja B:n ylläpitämä. Pilvipalvelun tuottaja B lupaa vahvan salauksen sekä monipuoliset varmistusratkaisut varmistamaan, että asiakkaiden tietoaineistot ovat turvassa ja aina saatavilla. Asiakas voi myös itse määritellä, suunnitella ja rakentaa pilven arkkitehtuurin kuten palvelinten, verkkojen sekä palomuurien arkkitehtuurit ja säännöstöt niin turvalliseksi kuin haluaa ja tarvittaessa pilvipalvelun tuottaja B auttaa tietoturvan määrittelyssä.

Pilvipalvelun tuottaja B tarjoaa alustaratkaisuksi myös Microsoft Cloud Platform -alustaa, joka mahdollistaa perustamaan yksityisen pilven kun vaatimuksena ovat korkeat kontrolli- ja tietoturvavaatimukset. Pilvialusta on myös yhteensopiva Microsoft Azuren kanssa, joka helpottaa siirtämään työkuormia pilvialustan ja Azuren välillä. Pilvialusta voidaan integroida tarvittaessa myös osaksi asiakasorganisaation omaa tietoverkkoa.

Pilvipalveluissa kaikki hallintayhteydet ovat vahvasti salattuja. Pilvipalvelun tuottaja B lupaa, että heidän ylläpitäjät eivät pääse asiakkaan tietoaineistoihin käsiksi. Myös jokai-

nen asiakas on virtuaaliympäristössä erotettu Kernel-based Virtual Machine (KVM)-teknologialla omaan ympäristöön.

Pilvipalvelun tuottaja B käyttää teknistä tietoliikenteen valvontaa ympärivuorokautisesti poikkeamien havaitsemiseksi tietoliikenteessä useilla eri OSI-tasoilla. Verkkohyökkäyksen tapahtuessa tietoliikenne ohjataan muualle muuttamalla esimerkiksi BGP-protokollan reititystietoja, nimipalvelutietoja tai molempia.

Pilvipalvelun tuottaja B ei tue muun muassa IBM:n kehittämää Trusted Platform Module -teknologiaa virtuaalilaite-alustoilla lisäämään muistin ja suorituksen aikaista tietoturvaa. Sen sijaan B mahdollistaa hyödyntämään SafeNet ja Trend Micron tietoturvaratkaisuja heidän pilvipalvelun alustoilla.

Tämän lisäksi pilvipalvelun tuottaja B lupaa:

- Palvelinkohtaiset palomuurit
- Verkkoteknologia, joka tekee turvallisten monikerroksisten verkkojen rakentamisesta helppoa
- Saatavuusalueilla kahdennetut yhteydet pilvipalvelun tuottaja B:n runkoverkkoon ja FICIX (Finnish Communication and Internet Exchange)-solmuun
- Tarvittaessa saatavilla kattavat tietoturvapalvelut, esimerkiksi vaikka palvelunestohyökkäyksiltä suojautumiseen
- Valmiit CLI, API ja SDK (.NET, Java, Node.js, Ruby, PHP, Python) rajapinnat ja työkalut
- SDN-verkkoteknologia (ohjelmallisesti määriteltävät verkot)
- Object ja Block tiedontallennus
- Amazon S3 yhteensopiva rajapinta
- Pilvipalvelun tuottaja B pilvialustasta osaksi asiakkaan yritysverkkoa

Analyysi pilvipalvelun tuottaja B:stä:

Pilvipalvelun tuottaja B:n osalta voidaan saatavilla olevan materiaalin pohjalta päätellä, että he ovat panostaneet palvelun saatavuuteen ja fyysiseen suojaustasoon muun muassa

vikasietoisella runkoverkolla ja valvomalla tietoliikenneyhteyksiä OSI-mallin eri kerroksilla.

Pilvipalvelun tuottaja B on toteuttanut kuten myös A infrastruktuuri- ja sovellustietoturvan suojaamiseksi teknisiä toimenpiteitä muun muassa valvontaa tunnistamaan verkkohyökkäyksiä sekä syvyyspuolustustekniikoita suojaamaan luvatonta tunkeutumista vastaan. Lisäksi voidaan päätellä, että B kerää lokitietoja koska valvoo verkkoinfrastruktuuria OSI-mallin eri kerroksilla. Sen sijaan B:n osalta ei voida päätellä säännöllisiä sovellusten haavoittuvuus-skannauksia.

Pilvipalvelun tuottaja B:stä kerätyn materiaalin pohjalta voidaan päätellä myös, että he ovat panostaneet datan suojaukseen ja elinkaarenhallintaan toisin kuin A ja C koska noudattavat VAHTI, KATAKRI ja PCI DSS ohjeita ja standardeja. Tämän lisäksi B:llä on ISO/IEC 27001 sertifikaatti osoituksena tietoturvallisuuden hallintajärjestelmien tietoturvasta.

Edellä mainittujen ohjeiden ja standardien noudattamisella voidaan lisäksi päätellä, että pilvipalvelun tuottaja B on suojannut infrastruktuuri- ja sovellustietoturvaa, pääsynvalvontaa, avainten hallintaa riittävällä tasolla. Toisin kuin C:n osalta analyysissa ei voida päätellä mitään avainten hallinnan sekä datan suojauksen ja elinkaarenhallinnasta. A:n osalta avainten hallinta voidaan päätellä siltä osin kuin he noudattavat symmetristä salausta, joka on hoidettu asiakkaan toimesta.

VAHTI ja KATAKRI ohjeiden noudattamisella voidaan edelleen päätellä, että pilvipalvelun tuottaja B on huolehtinut datan maantieteellisen sijaintivaatimuksen, menettelyohjeet on toteutettu tunnuksille ja niiden käsittelylle sekä menettelyohjeet miten käsitellään tietoaineistoa pilvipalvelussa. Myös tietoaineistoa siirrettäessä tai tallennettaessa pilvipalveluun suojataan riittävällä tasolla.

Pilvipalvelun tuottaja B kuten myös C mahdollistavat, että heidän pilvipalveluun voidaan toteuttaa hybridimallin pohjalta pilviratkaisu, joka noudattaa asiakkaan vaatimusten mukaista tietoturvatasoa suojata tietoaineistoa pilvipalvelussa. Pilvipalvelun tuottaja B:n tietoturvaa voidaan parantaa myös hyödyntämällä SafeNetin ja Trend Micron tieto-

turvaa parantavia ratkaisuja, jotka mahdollistavat muuan muassa tehostamaan pääsynvalvontaa, avainten hallintaa ja yksityisyyden suojaa pilvipalvelussa. Sen sijaan pilvipalvelun tuottaja B ei tue IBM:n alun perin kehittämää Trusted Platform Module –teknologiaa.

6.3 Suomalainen pilvipalvelun tuottaja C

Pilvipalvelun tuottaja C:n datakeskukset sijaitsevat Suomessa, joka tarjoaa asiakkailleen IaaS-, PaaS- ja SaaS-pilvipalveluita kuten alustaratkaisuja, varmistuspalveluita asiakasyrityksen omalle tai ulkoistetulle palvelintilalle, sähköposti- ja virustorjuntapalveja.

Pilvipalvelun tuottajan C infrastruktuuri perustuu VMware Cloud -teknologiaan koska heidän mukaan WMware-tuotteet ovat paras ratkaisu kriittisten ja yksilöityjen pilvipalveluiden tuottamiseksi. Asiakkaille toimitetaan VMware-teknologialla toteutettu virtuaaliympäristö, joka on rajattu WMware-virtualisointikerrokseen. Virtuaaliympäristö mahdollistaa jaettujen ja yksityisten kapasiteettipalvelujen tarjoamisen asiakkaille sekä myös hybridi-mallin. Asiakkaat voivat ottaa palvelun resursseihin etäyhteyden käyttämällä vSphere-clientia tai web-pohjaista hallintapaneelia. Asiakkailla on täydet oikeudet virtuaaliympäristön ylläpitoon kuten asentamiseen, päivittämiseen ja virtuaalipalvelimien käynnistämiseen.

Pilvipalvelut suunnitellaan ja toteutetaan asiakkaiden tarpeiden ja vaatimusten mukaisesti kuten kapasiteettipalvelut ja tietoturva. Julkisen käyttöönottomalliin perustuvat palvelut toteutetaan muuttuvien kapasiteettitarpeiden mukaisesti ja yksityisen käyttöönottomallin mukaiset pilvipalvelut suunnitellaan korkeiden tietoturvavaatimusten mukaisesti. Hypridi-käyttöönottomallin mukaisesti asiakkaat voivat tarvittaessa myös laajentaa oman konesalikapasiteetin ulkoistamalla esimerkiksi liiketoimintakriittiset palvelut varmennettuun pilvipalveluun.

Asiakkaat voivat perustaa SSL-VPN -yhteydellä turvallisen etäyhteyden pilvessä oleviin tietojärjestelmiin. VPN-palvelu on käytettävissä myös erikseen asennettavalla asiakassovelluksella. Autentikaatiossa voidaan käyttää myös mobiilivarmennetta, jossa käyttäjä tunnistautuu yrityksen verkkoon mobiilivarmenteella, eli kännykkään lähetettä-

vällä kertakäyttöisellä ja uniikilla tunnuksella, joka parantaa palvelun tietoturvallisuutta entisestään.

Pilvipalvelun tuottaja C käyttää varmistuspalveluissa EMC:n varmistusperheen tuotteita. Pilvipalvelun tuottaja C tarjoaa etävarmistusta, jossa yritykset voivat varmentaa ulkoisille tallennuslaitteille tietoaineistot suojautuakseen mahdollisilta tietoturvakatastrofeilta. Palvelinten etävarmistukset voidaan kahdentaa kahteen maantieteellisesti erotettuun konesaliin, jolloin tiedon varmennus on vielä korkeammalla tasolla. Asiakasyrityksen konesaliin sijoitetaan deduplikoivan etävarmistusjärjestelmän laitteisto, joka toimii varmistuskohteena asiakkaan olemassa olevalle varmistussovellukselle. Laitteisto suorittaa deduplikointivertailun, minkä jälkeen se replikoi tuoreimmat uudet tiedot pilvipalvelun tuottajan C konesalissa sijaitsevaan varmistusjärjestelmään.

Pilvipalvelun tuottaja C mahdollistaa alustaratkaisun kaikille ohjelmistotaloille, toiminnanohjausjärjestelmille ja vastaaville ratkaisuille sekä ohjelmistoja tarjoaville yrityksille. Pilvipalvelun tuottaja C:n mukaan heidän alustaratkaisun tietoturva on korkeaa tasoa ja pilvialustan tietoturvaa suojataan F-Securen tietoturvaratkaisulla.

Pilvipalvelun tuottaja C käyttää datakeskusten tietoliikenneverkkojen toteutuksissa Juniperin laitteistoja, jossa tietoliikennelaitteiden välisissä yhteyksissä sekä pilvipalvelualustojen määrityksissä käytetään aina 10 Gbps liitäntöjä. Juniper EX -sarjan tietoliikennekytkimet tukevat niin sanottua virtuaalista kehikkotekniikkaa (Virtual Chassis), mikä mahdollistaa useiden kytkimien hallinnan yhtenä loogisena laitteena. Tällöin ylläpito yksinkertaistuu ja hallintakustannukset pienenevät. Lisäksi on voitu luopua Spanning Tree -protokollan käyttämisestä, mikä parantaa entisestään konesalien käytettävyyttä. Pilvipalvelun tuottaja C:n mukaan laiterikkojen tapahtuessa varayhteyksien käyttöönottoviive on millisekuntien luokkaa.

Datakeskusten konesaliverkot kulkevat aina palomuurien kautta, joissa palomuurilaitteistona käytetään Juniper SRX-sarjan laitteita. Palomuuripalvelut tuotetaan oletusarvoisesti ensisijaiseen konesaliin toteutusta vikasietoisesta SRX-palomuuriklusterista. Lisäksi pilvipalvelun tuottaja C on toteuttanut erittäin kriittisiä järjestelmiä varten erillisen maantieteellisesti kahdennetun SRX-palomuuriklusterin, jonka avulla on mahdollis-

ta tuottaa samoja muun muassa julkisen verkon ip-osoitteita itsenäisesti suoraan molemmista konesaleista.

Kiinteiden kahden pisteen välisten tietoliikenneyhteyksien määrittäminen VPN:llä onnistuu turvallisesti parhaaksi havaittuja sääntöjä noudattamalla. Palomuuri on laajennettavissa tunkeutumisen havainnointi- ja estojärjestelmällä (Intrusion Prevention System).

Datakeskusten konesalien väliset tietoliikenneyhteydet on toteutettu kahdennetuilla dedikoiduilla kuituyhteyksillä hyödyntämällä Dense Wavelength Division Multiplexing (DWDM) -tekniikkaa, joka mahdollistaa usean eri aallonpituuden kuljettamisen valokuitukaapeleissa. Internet-yhteydet on toteutettu usean operaattorin pääliittymillä (IP-transit), jotka on liitetty toisiinsa Border Gateway -protokollaa (BGP) käyttämällä.

Verkkoliikenteen kuormantasaajana pilvipalvelun tuottaja C käyttää F5 Big-IP kuormantasaajaa. F5 Big-IP kuormantasaaja mahdollistaa http-kyselyjen kasvaessa ohjaamaan liikenteen kuormantasaajalle määriteltyjen sääntöjen mukaan clusterissa toisille nodeille (sovelluspalvelimelle). Tietoliikennettä voidaan kontrolloida ja ohjata esimerkiksi vasteaikojen perusteella.

Analyysi pilvipalvelun tuottaja C:stä:

Pilvipalvelun tuottaja C:n osalta voidaan päätellä, että he ovat toteuttaneet infrastruktuuri- ja sovellustietoturvan osalta toimenpiteitä suojata pilvipalvelua ulkoisilta hyökkäyksiltä ja tunkeutumisyrityksiltä. C:n osalta voidaan lisäksi päätellä, että he tekevät säännöllisiä haavoittuvuus-skannauksia koska suojaavat infrastruktuuria F-Securen tietoturvaratkaisuilla.

Pilvipalvelun tuottaja C:n materiaalin pohjalta voidaan lisäksi päätellä, että he ovat laajentaneet tietoaineiston siirron aikaista suojausta sekä virtuaalilaitteiden ilmentymien suojausta siirrettäessä tietoaineistoa tietoverkkojen ja hypervisoreiden välillä. He mahdollistavat myös asiakkaan käyttämään avoimia salausmenetelmiä siirrettäessä tietoaineistoa asiakkaan ja pilvipalvelun välillä.

Toisaalta pilvipalvelun tuottaja C ei kerro www-sivuillaan noudattavansa VAHTI-, KATAKRI-ohjeiden suosituksia tai onko organisaatiolla IEC/ISO 27001 sertifikaattia pilvipalveluiden tietoturvan varmistamiseksi. Pilvipalvelun tuottaja C vakuuttaa kuitenkin www-sivuillaan, että heidän alustaratkaisunsa tietoturva on korkeaa tasoa ja sitä suojataan F-Securen tietoturvaratkaisulla. Tämän lisäksi koska C:n pilvialustan arkkitehtuuri perustuu WMware-teknologiaan voidaan tietoturvaa tarvittaessa parantaa SafeNetin ja Trend Micron tietoturvaratkaisuilla. Sen sijaan ei ole tietoa voidaanko hyödyntää Trusted Platform Module –teknologiaa parantamaan pilvialustojen tietoturvaa.

Pääsynvalvonnan osalta C kertoo www-sivuillaan estäneensä oikeudettoman pääsyn asiakaan tietoihin sekä myös valvoo tämän toteutumista. Pilvipalvelun tuottaja C kertoo www-sivuillaan myös suojaavansa asiakkaan tietoliikenneyhteyksiä SSL-VPN-ratkaisulla ja tietoturvaa voidaan edelleen parantaa käyttäjän vahvalla todentamisella muun muassa käyttämällä mobiilivarmenteita.

Pilvipalvelun tuottaja C on panostanut pilvipalvelussa saatavuuteen muun muassa parantamalla tietoliikenneyhteyksien vikasietoisuutta sekä tarjoamalla asiakkailleen monipuolisia tietoaineiston varmistuspalveluja.

6.4 Kyselytutkimuksen tulokset

Tässä työssä selvitettiin case-tutkimuksen pohjalta pilvipalveluiden tietosuojaa Suomessa. Tiedot pilvipalveluiden tuottajien tietoturvasta kerättiin julkisilta www-sivuilta sekä kyselytutkimuksella, jossa on kysymyksiä yhteensä 69 kohdistuen kuuteen tietoturvan ja tietosuojan teema-alueeseen pilvipalvelun infrastruktuuri- ja sovellustietoturvaan, datan suojaus, luokittelu ja elinkaarenhallintaan, salausavainten hallintaan, pääsynvalvontaan, lokien valvontaan ja tunkeutumisen estämiseen sekä tietoturva-standardien noudattamiseen ja vaatimustenmukaisuuteen IaaS-, PaaS- ja SaaS-palveluissa. Katso liite 1.

Kyselytutkimus kohdistettiin kolmelle suomalaiselle pilvipalvelun tuottajalle joidenka datakeskukset sijaitsevat Suomessa ja noudattavat Suomen lainsäädäntöä. Valitettavasti kyselytutkimus koettiin laajaksi ja kysymykset liian yksityiskohtaisiksi, joten tässä opinnäytetyössä ei voitu luotettavasti selvittää suomalaisten pilvipalveluiden tietoturvan

ja tietosuojan tasoa aukottomasti kyselytutkimuksella. Kysymysten supistamisella ja yleistämisellä ei olisi voitu selvittää riittävällä tarkkuudella tietosuojan tasoa.

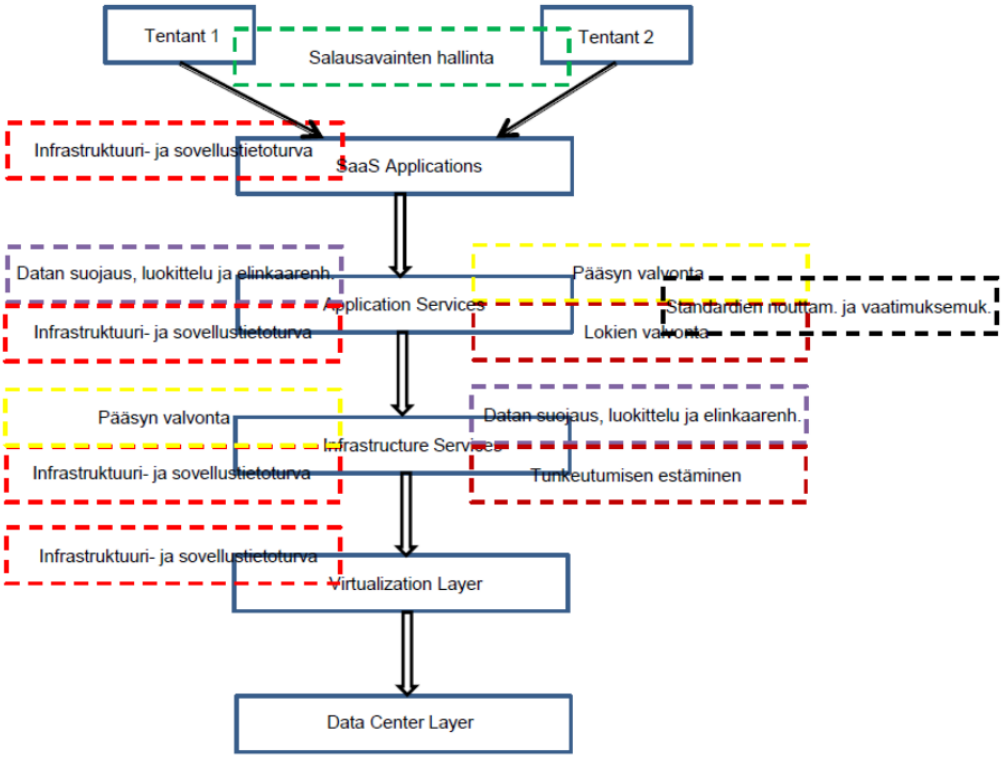
Tässä työssä ei voida siten käsitellä tuloksia analyyttisesti esimerkiksi jollakin tilastollisella menetelmällä koska tämä olisi edellyttänyt riittävän laajaa vastauksien määrää. Suomalaisten pilvipalvelun tuottajien www-sivuilta kerätystä materiaalista kuitenkin voidaan päätellä yleisellä tasolla tietoturvasta mutta ei riittävällä tarkkuudella johtopäätösten tekemiseksi tietosuojan tasosta varmistaa tietoaineistoa pilvipalvelussa.

Kuvassa 21 on ryhmiteltynä kyselytutkimuksen kuusi teema-aluetta Subashini *et al.* 2011 tietoturvatasoihin SaaS-pilvipalvelumallissa. Katso kuva 8 sivulla 19 Subashini *et al.* SaaS-pilvipalvelumallin tietoturvatasot. Seuraavassa on analysoitu miten kolme pilvipalveluntuottajaa A, B ja C ovat sijoittuneet kuvan 21 malliin julkisten www-sivujen pohjalta tehdyn case-analyysin perusteella.

Pilvipalvelun tuottajat A, B ja C sijoittuvat kuvan 21 mallissa infrastruktuuri- ja sovellustietoturvan osalta Application Services ja Infrastructure Services tietoturvatasoille. Kaikki kolme palveluntuottajaa ovat toteuttaneet tekniikkaa suojaamaan ja havaitsemaan ympäristössä tapahtuvat ulkoiset hyökkäys- ja tunkeutumisyritykset.

Tämän lisäksi pilvipalvelun tuottaja C sijoittuu infrastruktuuri- ja sovellustietoturvan osalta Vitualization Layer tasolle koska he ovat laajentaneet tietoaineiston siirron aikaista suojausta sekä virtuaalilaitteiden ilmentymien suojausta siirrettäessä tietoaineistoa tietoverkkojen ja hypervisoreiden välillä.

Datan suojauksen, luokittelun ja elinkaaren osalta pilvipalvelun tuottaja A ja C eivät sijoitu kuvan 21 mallin mukaan Application Services ja Infrastructure Services tietoturvatasoille koska case-analyysissä käytetyn julkisen materiaalin pohjalta tätä ei voida todentaa. Sen sijaan B:n osalta tämä voidaan päätellä koska he noudattavat suomalaisten viranomaisten tietoturvasuosituksia ja –ohjeita.



Kuva 21. *Kyselytutkimuksen teemat ryhmiteltynä Subashinin et al. tietoturvatasoihin.*

Salausavainten hallinnasta voidaan A:n ja B:n osalta päätellä kuvan 21 mallissa, että asiakas kontrolloi itse salausavaimia. Sen sijaan C:n osalta tätä ei voida käytetyn materiaalin pohjalta todentaa. Pääsyn valvonnan osalta voidaan päätellä, että pilvipalvelun tuottaja C sijoittuu kuvan 21 mallissa Application Services tietoturvatasolle, koska he kertovat www-sivuillaan estäneensä oikeudettoman pääsyn asiakaan tietoihin sekä myös valvovat tämän toteutumista. Myös B:n osalta tämä voidaan päätellä koska noudattavat suomalaisten viranomaisten tietoturvaohjeita ja suosituksia sekä standardeja.

Tunkeutumisen estämisen osalta voidaan päätellä, että kaikki analyysin pilvipalvelun tuottajat A, B ja C sijoittuvat mallin Infrastructure Services tietoturvatasolle. Lokien valvonta sijoittuu mallissa Application Services tietoturvatasolle. Tälle tasolle voidaan päätellä sijoittuvan sekä A:n että B:n. C:n osalta tätä ei voida päätellä.

Standardien noudattamisen ja vaatimuksen mukaisuus sijoittuu Subashinin *et al.* mallissa Application Services tietoturvatasolle. Tälle tietoturvatasolle mallissa sijoittuu julkisen materiaalin pohjalta pilvipalvelun tuottaja B. Muiden osalta tätä ei voida päätellä.

7 JOHTOPÄÄTÖS

Tässä diplomityössä haettiin vastausta seuraaviin tutkimuskysymyksiin:

- Miten hyvin tutkittavien suomalaisten pilvipalveluja tarjoavien toimijoiden tietoturvaan liittyvät ratkaisut turvaavat arkaluonteisen tietoaineiston pilvessä?
- Millaisia mahdollisuuksia on pilvipalvelua hyödyntävällä asiakkaalla varmistua ja kontrolloida itse pilveen tallennetun tietoaineiston tietosuojasta?
- Miten paljon tutkittavat pilvipalvelun tuottajat hyödyntävät ja noudattavat tietoturvastandardeja arkaluontoisen tietoaineiston suojaamiseksi pilvessä?

Kaikki case-tutkimuksen A, B ja C pilvipalvelun tuottajat ovat investoineet palvelun fyysiseen suojaamiseen, palvelun käytettävyyteen ja saatavuuteen. Myös voidaan päätellä infrastruktuuri- ja sovellustietoturvan, lokien valvonnan ja tunkeutumisen estämisen olevan hyvällä tasolla. Datan suojauksen, luokittelun ja elinkaarenhallinnan sekä salausavainten hallinnan osalta tässä työssä ei voida päätellä suojausta.

Tässä työssä ei voida myöskään päätellä ja saada vastausta tutkimuskysymyksiin, miten hyvin asiakkaan tietoaineistoa suojataan palvelussa ja voiko asiakas itse kontrolloida tietoaineiston suojaa luvattomalta urkinnalta, kopionilta, käytöltä ja niin edelleen tietosuojan varmistamiseksi. Myöskään kaikkien case-tapausten osalta ei voida arvioida standardien ja ohjeiden noudattamista ja miten hyvin tietoturvaan liittyvät menettelyohjeet on dokumentoitu.

Vaikka tässä työssä ei saatu kyselytutkimuksella vastauksia case-tapausten tietoturvatasosta voidaan suomalaisten pilvipalvelun tuottajien B ja C osalta päätellä, että heidän pilvipalveluiden tietoturvaa voidaan tehostaa ja parantaa hyödyntämällä tämän työn luvussa 5.2 esitettyjä tietoturvaratkaisuja.

Hyödyntämällä luvussa 5.2 esitettyjä SafeNetin ja Trend Micron tietoturvaratkaisuja voidaan tietoturvaa parantaa seuraavilla osa-alueilla: infrastruktuuri- ja sovellustieto-

turva, datan suojaus, luokittelu ja elinkaarenhallinta, salausavainten hallinta, pääsynvalvonta, lokien valvonta ja tunkeutumisen estäminen.

Työn teoreettisen viitekehyksen sekä kerätyn julkisen materiaalin pohjalta voidaan päätellä, että tietosuojan parantamisen ja kehittämisen näkökulmasta suomalaisten pilvipalveluiden tuottajien tulee kiinnittää enemmän huomioita ja noudattaa suomalaisten tietoturvaviranomaisten antamia määräyksiä ja ohjeita sekä standardeja tarjottaessa pilvipalveluita. Myös havaintona voidaan tehdä, että tässä työssä tutkituista pilvipalveluiden tuottajista ei heidän julkisen materiaalin pohjalta voida päätellä tukevatko he kolmannen osapuolen tekemiä auditointeja tai mahdollistavatko he suojaamaan infrastruktuuria ulkoisilta uhilta hyödyntämällä esimerkiksi Trusted Platform Module –teknologiaa tietosuojan parantamiseksi pilvipalveluissa.

LÄHTEET

Amazon. (2014). Saatavissa: http://aws.amazon.com/s3/.

Armbrust, M., Fox, A., Griffith, R., Joseph A.D., Katz R.H., Konwinski A., Lee, G., Patterson D.A., Rabkin A., Stoica I. & Zaharia M. (2009). Above the Clouds: A Berkeley view of cloud computing. (Technical Report UCB/EECS-2009-28), University of California at Berkeley, Electrical Engineering and Computer Sciences. Saatavissa: http://www.cs.columbia.edu/~roxana/teaching/COMS-E6998-7-Fall-2011/papers/armbrust-tr09.pdf.

Bajpai, S. & Srivastava, P. (2014). A Fully Homomorphic Encryption Implementation on Cloud Computing. International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 811-816.

Blakley, G. R. (1979). "Safeguarding cryptographic keys". Proceedings of the National Computer Conference 48: 313–317.

Bode, S., Fischer, A., Kühnhauser, W. & Riebisch, M. (2009). Software Architectural Design Meets Security Engineering. Saatavissa: http://www.researchgate.net/publication/220882839_Software_Architectural_Design_Meets_Security_Engineering.

Brakerski, Z. & Vaikuntanathan, V. (2011). Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. In: Advances in Cryptology- Proceedings of CRYPTO'11, Lecture Notes in Computer Science (LNCS), Vol 6841, Springer-Verlag, pp. 505-524.

Brakerski, Z. & Vaikuntanathan, V. (2011a). Efficient Fully Homomorphic Encryption from (Standard) LWE. In: Proceedings of the IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS'11), pp. 97-106, ACM Press, New York, NY, USA.

Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2011). Fully Homomorphic Encryption without Bootstrapping. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS'12), pp. 309-325, ACM Press, New York, NY, USA.

Brickell, E. F. & Yacobi, Y. (1987). On Privacy Homomorphisms. In: Advances in Cryptology – Proceedings of EUROCRYPT 1987, Lecture Notes in Computer Science (LNCS) Vol 304, Springer-Verlag, pp. 117-125.

Brunette, G. & Mogull, R. (2009) "Security guidance for critical areas of focus in cloud computing", CloudSecurityAlliance.

CareStream Health. (2011). How to Evaluate the Data Security Capabilities of Cloud-Based Services. Saatavissa: http: //www.carestream.com/WhitePaper_Cloud-Security.pdf.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. & Molina, J.(2009). Controlling data in the cloud: outsourcing computation without outsourcing control. Proceedings of the ACM Workshop on Cloud Computing Security. Saatavissa: http://www.parc.com/content/attachments/ControllingDataInTheCloud-CCSW-09.pdf.

Cloud Security Alliance (CSA). (2014). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. Saatavissa: http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

Common Criteria. (2015). Saatavissa: http://www.commoncriteriaportal.org/cc/

Coron, J.-S., Mandal, A., Naccache, D., & Tibouchi, M. (2011). Fully Homomorphic Encryption over the Integers with Shorter Public Keys. In: Advances in Cryptology -

Proceedings of CRYPTO'11, Lecture Notes in Computer Science (LNCS), Vol 6841, Springer-Verlag, pp. 487-504.

Dey, M. (2007). Information security management - a practical approach. In Proceedings of AFRICON 2007 Windhoek, Republic of Namibia, September 26-28 (s. 1-6).

Federal Information Processing Standards Publications. (2001). ADVANCED ENCRYPTION STANDARD (AES). Saatavissa: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

Furukawa, J., Furukawa, R., Mori, T., Mori, K., Isshiki, T. & Araki T. (2013). A Privacy-Protection Data Processing Solution Based on Cloud Computing. Vol. 8. NEC Technical Journal.

Gadzheva, M. (2008). Privacy in the Age of Transparency: The New Vulnerability of the Individual. Social Science Computer Review. Saatavissa: http://propid.ischool.utoronto.ca/wp-content/uploads/2011/05/gadzheva.pdf.

Gentry, C. (2009). A fully homomorphic encryption scheme. PhD thesis, Stanford University.

Gentry, C. (2010). Computing arbitrary functions of encrypted data, Commun. ACM, Vol. 53, No. 3., pp. 97–105.

Gentry, C. & Halevi, S. (2011). Implementing Gentry's Fully-Homomorphic Encryption Scheme. In: Advances in Cryptology - Proceedings of EUROCRYPT'11, Lecture Note in Computer Science (LNCS), Vol 6632, Springer-Verlag, pp. 129-148.

Gentry, C., Halevi, S. & Smart, N.P. (2012). Fully homomorphic encryption with polylog overhead. In Proceedings of the 31st Annual international conference on Theory and Applications of Cryptographic Techniques, EUROCRYPT'12, pages 465–482, Berlin, Heidelberg, 2012. Springer-Verlag.

Gentry, C, Halevi, S., & Smart, N. (2012). Better Bootstrapping in Fully Homomorphic Encryption. In: Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography (PKC'12), Lecture Notes in Computer Science (LNCS), Vol 7293, Springer-Verlag, pp. 1-16.

GlobalPlatForm. (2015). Saatavissa: https://www.globalplatform.org/mediaguidetee.asp

Green, L. (2007). Service level agreements: an ontological approach. University of Technology, Sidney. NSW, Australia. Saatavissa: http://www.researchgate.net/publication/221550192_Service_level_agreements_an_ontological_approach.

Hakala, M., Vainio, M. & Vuorinen, O. (2006). Tietoturvallisuuden käsikirja. Kustantaja:Docendo. ISBN:9789518462739

Harrington, A. & Jensen, C.D. (2003). Cryptographic Access Control in a Distributed File System. Department of Computer Science Trinty College Dublin. Saatavissa: https://www.cs.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-28.pdf.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (1997). Tutki ja kirjoita. Helsinki:Kirjayhtymä.

IDC. (2014). Saatavissa: http://www.idc.com.

Itani, W. & Kayssi, A. (2009). Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures. 8th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Chengdu, China.

ISO. (2015). Saatavissa: http://www.iso.org/iso/home.htm.

ITIL. (2015). Saatavissa: https://www.axelos.com/best-practice-solutions/itil

Jensen, M., Schwenk, J., Gruschka, N. & Lo Iacono, L. (2009). On Technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing, Ban-

galore, India, 21 September 2009 through 25 September 2009. ISBN: 978-076953840-2. Scopus.

Järvinen, P. (2003). Salausmenetelmät. Porvoo: Docendo Finland Oy.

Järvinen, P. (2010). Yksityisyys: Turvaa digitaalinen kotirauhasi. Jyväskylä: WSOYpro.

KATAKRI. (2011). Kansallinen turvallisuusauditointikriteeristö. Saatavissa: http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf.

Kaufman, L.M. 2009. Data Security in the World of Cloud Computing. IEEE Security & Privacy Magazine. Vol. 7.

Kauffman, R.J. & Tsai, J.Y. (2010). With or without you: The countervailing forces and effects of process standardization. Electronic Commerce Research and Applications.

Kellerman, T. (2010). Cyber-Threat Proliferation: Today's Truly Pervasive Global Epidemic. Security & Privacy, IEEE. Saatavissa: http://www.coresecurity.com/files/attachments/ieee.kellermann.05.10.pdf.

Dijk, M., Gentry, C., Halevi, S. & Vaikuntanathan, V. (2010). Fully Homomorphic Encryption over the Integers. Eurocrypt 2010.

Mei, H., Dawei, J., Guoliang, L. & Yuan, Z. (2009) "Supporting Database Applications as a Service", ICDE'09:Proc. 25thIntl.Conf. on Data Engineering, pp. 832-843.

Mermin, N.D. (2006). Breaking RSA Encryption with a Quantum Computer - Shor’s Factoring Algorithm. Cornell University, Physics 481-681, CS 483. Saatavissa: http://web.archive.org/web/20121115112940/http://people.ccmr.cornell.edu/~mermin/qcomp/chap3.pdf.

Microsoft. 2014. Windows Trusted Platform Module Management Step-by-Step Guide. Saatavissa: http://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx.

Modi, C., Patel, D., Borisaniya, H., Patel, A. & Rajarajan, M. (2013). “A survey of intrusion detection techniques in Cloud,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57. Saatavissa: http://ac.els-cdn.com/S1084804512001178/1-s2.0-S1084804512001178-main.pdf?_tid=fdf241ac-d6eb-11e4-9910-00000aacb35f&acdnat=1427727159_60332baf73d429376af98a5bea8d313d

Mohta, A. & Awasthi, L.K. (2012). Cloud Data Security while using Third Party Auditor. International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012. ISSN 2229-5518.

Muthakshi, S., Phil, M., Meyyappan, T. & Phil, M. A. (2013). Survey on Security Services In Cloud Computing. International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue7- July 2013.

Naehrig, M., Lauter, K., & Vaikuntanathan, V. (2011). Can Homomorphic Encryption be Practical? In: Proceedings of the 3rd ACM Workshop on Cloud Computing Security, pp. 113-124, ACM Press, New York, NY, USA.

NIST. (2014). Saatavissa: http://www.nist.gov/itl/cloud/index.cfm.

OASIS. (2015). Saatavissa: https://www.oasis-open.org/standards

PCI. (2015). Saatavissa: https://www.pcisecuritystandards.org/security_standards/

Pervez, Z., Kyung H. & Sungyoung, L. (2010). Multi-Tenant, Secure, Load Disseminated SaaS Architecture. The 12th International Conference on Advanced Communication Technology (ICACT), February 7-10.

Pfleeger, C. & Pfleeger, S. (2006). Security in Computing. Fourth Edition. Pfleeger Consulting Group.

Rijmen, V. & Daemen, J. (1999). AES Proposal: Rijndael. Saatavissa: 1999http://www.science.upm.ro/~apetrescu/OLD/public_html/Tehnologia%20Informatiei/Securitatea%20informatiei/Laborator/AES/rijndael%20doc%20V2.pdf.

Rimal, B.P., Choi, E. & Lumb, I. (2009). A Taxonomy and Survey of Cloud Computing Systems. In Proceedings of 5th International Joint Conference on INC, IMS and IDC, Seoul, Korea, August 25- 27. Saatavissa: http://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CDsQFjAD&url=http%3A%2F%2Fvirtualcluster.googlecode.com%2Ffiles%2FA%2520Taxonomy%2520and%2520Survey%2520of%2520Cloud%2520Computing%2520System.pdf&ei=MEkhU9eZN8GBywO_sIK4Ag&usg=AFQjCNH45lY_HDxdFhcNcWM8gObfqcnb7g&bvm=bv.62922401,d.bGQ.

Ristenpart, T., Tromer, E., Shacham, H. & Savage, S. (2009). "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds", CCS'09: Proc. 16thACM Conf. on Computer and communications security, pp. 199-212.

Rivest, R., Adleman, L. & Dertouzos, M. (1978). On data banks and privacy homomorphisms. In Foundations of Secure Computation, pp. 169–180.

SafeNet. (2014). The Data protection company. WWW-dokumentti: http://www.safenet-inc.com/. Luettu: 13.10.2014.

Salo, I. (2011). Cloud computing – palvelut verkossa. Docendo.

Shamir, A. (1979). "How to share a secret". Communications of the ACM 22 (11): 612–613.

Shpantzer, G. (2013). Implementing Hardware Roots of Trust: The Trusted Platform Module Comes of Age. A SANS Whitepaper. PDF-dokumentti: http://www.trustedcomputinggroup.org/resources/implementing_hardware_roots_of_trust.

Smart, N. P. & Vercauteren, F. (2010). Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. In: Public Key Cryptography - Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography (PKC'10), Lecture Notes in Computer Science (LNCS), Vol 6056, Springer-Verlag, pp. 420-443.

Smart, N. & Vercauteren. (2012). Fully Homomorphic SIMD Operations. Design Codes and Cryptography, Springer, USA, July 2012.

Somea ICT Solutions. (2014). Saatvissa: http://colibrix.net/cloud/.

Sripanidkulchai, K., Sahu, S., Ruan, Y., Shaikh, A. & Dorai, C. (2010). Are clouds ready for large distributed applications? SIGOPS Operating Systems Review, 44(2). Saatavissa: http://www.cs.cornell.edu/projects/ladis2009/papers/sripanidkulchai-ladis2009.pdf.

Subashini, S. & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. Vol. 34. Academic Press Ltd.

Tafti, M. (2005). Risk factors associated with offshore IT outsourcing. Industrial Management & Data Systems, 105(5). 549–560.

Takabi, H., Joshi, J.B.D & Ahn, G. J. (2010) "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6), pp. 24-31.

Tilastokeskus. (2015). Saatavissa: http://www.stat.fi/til/icte/2014/icte_2014_2014-11-25_tie_001_fi.html

Trend Micro. (2014). SecureCloud - Securing and Controlling Sensitive Data in the Cloud. WWW-dokumentti: http://www.trendmicro.com/us/enterprise/cloud-solutions/secure-cloud/. Luettu: 16.10.2014.

Vaquero, L. M., Rodero-Merino, L., Caceres, J. & Lindner, M. (2009). A break in the clouds: towards a cloud definition. SIGCOMM Computer Communication Review, 39(1), 50-55.

VAHTI. (2012). Teknisen ICT-ympäristön tietoturvataso-ohje. Suomen yliopistopaino Oy.

Viestintävirasto. (2014). Saatavissa: https://www.viestintavirasto.fi/tietoturva/viestintavirastontietoturvapalvelut/ncsa-fi.html.

Viega, J. (2009). Cloud computing and the common man. pp. 106-108.

Wang, C., Sherman, S., Chow, M., Wang, Q., Ren, K. & Lou, W. 2013. Privacy-Preserving Public Auditing for Secure Cloud Storage. IEEE Trasaction on Computers I, vol. 62, no. 2, pp.362-375 , February 2013.

Wang, C., Wang, Q., Ren, K. & Lou, W. (2010). Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. IEEE INFOCOM 2010.

Wang, W., Li, Z. & Owens, R. (2009). Secure and efficient access to outsourced data. In Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW) Chicago, Illinois, USA, November 13. New York: ACM. Saatavissa: http://www.cs.iastate.edu/~wzhang/teach-552/ReadingList/552-16.pdf.

Wenliang, D. & Zhijun, Z. (2002). A practical approach to solve Secure Multi-party Computation problems. NSPW '02 Proceedings of the 2002 workshop on New security paradigms. ACM New York, NY, USA ©2002. ISBN:1-58113-598-X

Xu-Dong, W. & Xin, L. (2012). Protect Cloud Computing's Data Using Fully Homomorphic Encryption. National Conference on Information Technology and Computer Science (CITCS 2012).

Yao, A.C. (1982). Protocols for Secure Computations. University of California Berkeley, California 94720. Saatavissa: http://research.cs.wisc.edu/areas/sec/yao1982-ocr.pdf.

Youseff, L., Butrico, M. & Da Silva, D. (2008). Toward a Unified Ontology of Cloud Computing. In Proc. of Grid Computing Environments Workshop, (GCE08). Saatavissa: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.176.3634&rep=rep1&type=pdf.

Zhang, S., Zhang, S., Chen, X. & Wu, S. (2010). Analysis and Research of Cloud Computing System Instance. Second International Conference on Future Networks (ICFN), Sanya, Hainan, China, January 22-24 (s. 88-92). Los Alamitos: IEEE Computer Society.

Liite 1

LIITTEET

Kyselytutkimuksella kartoitettiin tavanomaisten (IaaS, PaaS, SaaS) pilvipalvelumallien tietosuojaa ja tietoturvaa.

Kyselytutkimuksessa pyydettiin arvioimaan organisaation datan suojaamiseen liittyvää tietoturvaa ja vastaamaan esitettyihin kysymyksiin. Kysymyksiä on yhteensä 69 ja ne on jaoteltu kuuteen tietoturvan ja tietosuojan teema-alueeseen. Arviointiasteikko Kyllä, Ei tai Ei tietoa.

Liite 1

	Tietoturvan ja tietosuojan arviointikysymykset	IaaS	Vastaukset			PaaS	Vastaukset			SaaS	Vastaukset		
			Kyllä	Ei	Ei tietoa		Kyllä	Ei	Ei tietoa		Kyllä	Ei	Ei tietoa
Infrastruktuuri- ja sovellustietoturva	*Käytätteko automaattisia lähdekoodin analysointityökaluja tietoturvahavaavoittuvuuksien havaitsemiseksi?*												
	Tarkistatteko sovellukset tietoturvahavaavoittuvuuksien osalta ja huomioite mahdolliset korjaukset tuotteeseen?												
	Ovatko kaikki pääsynvalvontaa koskevat vaatimukset ja luottamustasot määritelty ja dokumentoitu?												
	Oletteko toteuttaneet teknisiä toimenpiteitä ja syvyyspuolustustekniikoita (esim.tietoliikenne pakettien analysointia, liikenteen rajoittamista ja tietoturva-aukkojen tunnistamista) tunnistamaan ja vastaamaan verkkohyökkäyksiä vastaan?												
	Onko hyökkäykset, jotka kohdistuvat virtuaali-infraan estetty teknisellä valvonnalla?												
	Onko teillä mahdollisuutta havaita hyökkäykset, jotka kohdistuvat suoraan virtuaali-infraan (esim. shimming, Blue Pill, Hyper jumping jne.)?												
	Teettekö sovellusten havoittuvuus-skannauksia säännöllisesti hyödyntämällä standardien mukaisia hyviä käytäntöjä?												
Datan suojaus, luokittelu ja elinkaarenhallinta	*Onko datan eheyden tarkistusrutiinit toteutettu sovelluksiin ja tietokantoihin ehkäisemään manuaaliset tai järjestelmälliset käsittelyvirheet tai datan korruptoitumisen?*												
	Mahdollistatteko kyvyn tunnistaa virtuaalilaitteet lipukkeiden/metatiedon kautta (esim. lippukkeita voidaan käyttää rajoittamaan vieras käyttöjärjestelmien lataamasta/siirtämällä tietoa väärässä maassa)?												
	Onko mahdollista käyttää järjestelmän maantieteellistä sijaintia tunnistamistietona?												
	Voidaanko mahdollistaa asiakkaan pyynnöstä ja/tai ennakolta datan fyysinen tallennustilan sijainti?												
	Voitteko varmistua, että dataa, johon on määritelty maantieteellinen sijaintivaatimus, ei siirry määritellyn maantieteellisen sijainnin ulkopuolelle?												
	Mahdollistatteko avoimet salausmenetelmät (esim. Advanced Encryption Standard jne.) asiakkaalle kun dataa siirretään yli julkisen tietoverkon (internet)?												
	Hyödynnättekö avoimia salausmenetelmiä aina kun infrastruktuurin kompponentit kommunikoivat yli julkisen tietoverkon (esim. internet-pohjainen datan replikointi ympäristöstä toiseen)?												
	Ovatko menettelyohjeet toteutettu tunnuksille, käsittellylle ja aineistoille ja kohteille jotka sisältävät dataa?												
	Onko olemassa menettelyjä varmistamaan, että tuotanto dataa ei replikoida tai käytetä testiympäristöissä tai vastaavassa?												
	Ovatko vastuut koskien datan omistajuutta määritelty, dokumentoitu ja kommunikoitu?												
	Tuetteko turvallista arkistoitujen ja varmuuskopioitujen tietojen poistamista (esim. magnetoinnin poisto/salauksen pyyhkiminen) asiakkaan pyynnöstä?												
	Onko teillä julkistettua menettelytapaa poistuvalle palvelusopimukselle, sisältäen vakuutuksen tyhjentää kaikki asiakkaan data kun asiakas on lopettanut pilvipalvelun käytön?												
	Ovatko järjestelmä- ja verkkoympäristöt suojattu palomuurilla tai virtuaalisella palomuurilla varmistamaan arkaluontoisen datan suojauksen ja erottamisen?												
	Salaatteko asiakkan datan (levylle/muistiin) ympäristössänne?												
	Laajennatteko salausta suojaamaan dataa ja virtuaalilaitteiden ilmentymiä siirron aikana verkkojen ja hypervisoreiden välillä?												
	Annatteko pilvipalvelun käyttäjälle dokumentaation miten tulee ylläpitää tehtävien eriyttämistä pilvipalveluissa?												

Liite 1

Salausavainten hallinta	*Onko teillä salausavainten hallintapolitiikat, jotka sitovat avaimet henkilöön?*													
	Onko teillä mahdollisuutta asiakaskohtaisesti sallia luomaan uniikki salausavain?													
	Onko teillä dokumentoidut omistajuudet kussakin salausavainten elinkaaren vaiheessa?													
	Onko teillä mahdollisuutta hallinnoida asiakkaan puolesta salausavaimia?													
	Tuetteko asiakkaan generoimia salausavaimia tai sallitteko asiakkaiden salaamaan dataa henkilöllisyydellä ilman käyttöoikeutta julkisen avaimen varmenteeseen (esim. henkilöllisyyspohjainen salaus)?													
	Onko teillä dokumentaatiota, jossa määritellään salauksen ja avainten hallinnan politiikat, menettelytavat ja ohjeet?													
	Ylläpitääkö salausavaimia asiakas tai luotettu avainten hallitsija?													
	Tallennetaanko salausavaimet pilveen?													
	Onko teillä erillinen avainten hallinta ja avainten käyttö?													
Pääsynvalvonta	*Rajoitatteko monitorointia ja lokeihin pääsyä teidän tietoturvallisuuden hallintajärjestelmissä? (esim. hypervisor, palomuurit, haavoittuvuus-skannerit, verkon nuuskijat, ohjelmistorajapinnat jne.)*													
	Onko teillä valvontaa varmistamassa käyttöoikeuksien poistamista järjestelmistä kun käyttäjätiliä ei enää tarvita?													
	Käytättekö hallintayhteyden muodostamisessa käyttötarkoitukseen omistettua turvaverkkoa mahdollistamaan pääsyn pilven infrastuktuuriin?													
	Hallinnoitteko ja tallennettako kaikkien henkilöiden identtiteettitiedot joilla on pääsy IT infrastruktuuriin ja verkkoresursseihin, sisältäen henkilöiden käyttöoikeustason?													
	Onko olemassa valvontaa ehkäisemään oikeudettoman pääsyn asiakkaan sovelluksiin, ohjelmiin tai lähdekoodiin ja varmistettu, että oikeus on rajoitettu ainoastaan valtuutetulle henkilölle?													
	Oletteko dokumentoineet kuinka myönnätte ja hyväksytte käyttöoikedet pilvikäyttäjän dataan?													
	Onko teillä menetelmää kohdistaa pilvipalvelun tuottajan ja asiakkaan datan luokittelua käyttöoikeuksien valvontaan?													
	Vaaditteko käyttäjiltä ja ylläpitäjiltä vähintään vuosittaista kelpuutusta oikeuksien saamiseksi järjestelmiin?													
	Jaatteko käyttäjien oikeuksiin liittyvät korjaus- ja varmennusraportit asiakkaillenne, jos oikeudeton pääsy asiakkaan dataa on tapahtunut?													
	Onko käyttöoikeuksien oikea-aikainen kumominen tai muuttaminen järjestelmiin tai dataan tehty koskien käyttäjien statuksen muutosta organisaatiossa, alihankijoita, yhteistyökumppaneita tai kolmatta osapuolta?													
	Onko käyttöoikeuden muutokset aioittu sisällyttää työsuhteen päättymiseen, sopimukseen, työsuhteen muutoksiin tai siirtoon organisaation sisällä?													
	Käytättekö avoimia standardeja autentikointipalveluissa?													
	Tuetteko identiteetti federaatiota (Security Assertion Markup Language, Services Provisioning Markup Language, WS-Federation jne.) keinona käyttäjien autentikoinnissa tai valtuuttamisessa?													
	Onko teillä tietoturvapolitiikoiden täytäntöönpanoa esim. XACML (eXtensible Access Control Markup Language) asettamaan käyttöoikeuksissa voimaan alueelliset lait ja politiikkarajoitukset?													
	Onko teillä identiteetin hallintajärjestelmää (mahdollistaa asiakkaan datan luokittelun) mahdollistamaan sekä roolipohjaiset että kontekstipohjaiset oikeudet dataan?													
	Tuetteko asiakkaan vahvaa todentamista (sertifikaatit, tokenit, biotunnisteet jne.) pilvipalveluihin kirjautumisessa?													
	Sallitteko asiakkaan käyttää kolmannen osapuolen identiteetin varmistuspalveluja?													

Liite 1

	Tuetteko salasanan (minimi pituus, ikä, historia, monimutkaisuus) ja käyttäjätilin sulkemisessa (lukitusrajaa ja - kestoa) täytäntöönpano politiikoita?												
	Sallitteko asiakkaan itse määritellä salasanan ja käyttäjätilin sulkemista?												
	Tuetteko mahdollisuutta pakottaa ensimmäisen kirjautumisen yhteydessä muuttamaan salasanan?												
	Onko teillä mekanismia vapauttaa käyttäjätili kun se on lukkiutunut (esim. itsepalvelu sähköpostilla, määritelty haastekysymyksiä, manuaalinen käyttäjätilin vapautus)?												
	Onko palvelut, jotka voivat merkittävästi hallita virtuaalipartitioita (esim. sulkemista, kloonaamista jne.) asianmukaisesti rajoitettu ja valvottu?												
	Rajoitatteko henkilöstön käyttöoikeuksia kaikkiin Virtual Machine Monitor (VMM) hallintatoimintoihin tai virtualisoitujen järjestelmien hallintakonsoleihin perustuen minimioikeuksien periaatteeseen ja käytättekö teknisessä valvonnassa esim. kahden tekijän autentikointi, jäljitystä, ip-osoitteiden suodatusta, palomuureja ja TLS-suojausta hallintakonsoleihin?												
Lokien valvonta ja tunkeutumisen estäminen	*Onko tiedoston eheys (host) ja verkon tunkeutumisen tunnistus (IDS) työkalut otettu käyttöön helpottamaan oikea-aikaista tunnistamista?*												
	Onko pääsy fyysisiin ja loogisiin käyttöoikeuksien valvontalokeihin rajoitettu ainoastaan valtuutetuille henkilöille?												
	Säilytetäänkö valvontalokit keskitetysti?												
	Tarkistetaanko valvontalokeja säännöllisesti tietoturvapoikkeamien varalta (esim. automaattisilla työkaluilla)?												
	Lokitatteko ja hälytättekö mistä tahansa muutoksesta virtuaaliilaitteella riippumatta sen tilasta (esim. ei käytössä, pois käytöstä, ajossa)?												
	Monitoroitteko ja kerättekö lokitietoja etuoikeudellisesta pääsystä (ylläpitäjä) tietoturvallisuuden hallintajärjestelmiin?												
Tietoturva-standardit ja vaatimustenmukaisuus	*Voitteko osoittaa, että sääntöjen ja standardien asianmukainen huolellisuus kartoitus valvontaan/arkkitehtuureihin/prosesseihin on tehty?*												
	Käytättekö teollisuus-standardeja (Build Security in Maturity Model benchmarks, Open Group ACS Trusted Technology Provider Framework, National Institute of Standards and Technology (NIST) jne.) rakennettaessa tietoturvaratkaisuja pilvessä ylläpidettäville järjestelmille, ohjelmistoille sekä koko ohjelmistokehityksen elinkaaren ajan?												
	Onko tietoturva-arkkitehtuurit suunniteltu hyödyntämällä teollisuus-standardeja (esim. Common Data Security Architecture, Cloud Security Alliance Trusted Cloud Architectural Standard, FedRAMP, Continuous Asset Evaluation, Situational Awareness and Risk Scoring Reference Architecture Report (CAESARS)) ehkäisemään tietojen paljastumisen, muuttamisen ja tuhoamisen?												
	Noudatatteko rakenteisia datan nimiöinti-standardja esim. ISO 15489, Oasis XML hakemistoerittelyä, Cloud Security Alliance datatyyppi ohjetta?												
	Voitteko varmistaa, että kaikki teidän ohjelmistotoimittajat noudattavat teollisuus-standardeja tietoturvan varmistamiseksi järjestelmien ja ohjelmistojen kehityksessä?												
	Teettekö tietoturvaauditointeja säännöllisesti?												
	Annatteko auditointituloksia asiakkalle heidän pyynnöstä?												
	Onko teillä tietoturvallisuuden hallintajärjestelmien sertifikaatti ISO 27001?												
	Noudatatteko suomalaista lainsäädäntöä ja viranomaisten asettamia ohjeistuksia esim. KATAKRI II, VAHTI 3/2012 suojata yksityisyyttä ja tietoaineistoja pilvessä?												